PRT-CTRL-SE

Protege System Controller
Reference Manual

ICTProtege®

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2012. All rights reserved.

Publication Date: March 2012

Contents

Protege System 9

Introduction 9
System Controller 9
Features 9
Protege System Management Suite 9
Protege Modules 10
Firmware Versions 10

Menu Tree 11

Menu Reference 11
Menu Tree 11
Main Menu Chart 13
Installer Menu Chart 14

Area Control 15

Area Status Display 15
Area Security 16
Regular Arming 16
Force Arming 17
Stay Arming 17
Disarming 18
24HR Enabling 18
24HR Disabling 19
Area Group Arming 19
Area Group Disarming 20
Arming Failure 20

Users 22

User Programming 23
Menu Groups 30
Area Groups 35
Door Groups 36
Access Level 39
User Status 43
Elevator Groups 44
Floor Groups 46

Events 49

Event Review 49

Hex Review 50
Statistics 50

Modules 52

LCD Keypad 52
Zone Expander 59
PGM Expander 61
Reader Expander 63
Analog Expander 84

Zone Inputs 88

Zone 88
Trouble Zone 94
Zone Type 99

PGM Outputs 108

Selecting a PGM to Modify 108

Area 111

Selecting an Area to Modify 111

Access Control 129

Door 129
Door Type 138
Elevator 141
Floor 144

Group 145

PGM Group 145
Keypad Group 147

Reporting 149

Services 149
Contact ID Reporting Service 151
Monitor Phone Service 157
Protege SMGT Service 159
Serial Printer Service 163
SIA Level 2 Reporting Service 165
AMX Home Automation Service 171
DVAC (Surgard) Reporting Service 171
ModBUS Slave Service 175
ModBUS Remote Reporting Service 178

Clipsal C-Bus Automation 179
Intercom High Level Interface 181
GSM Modem Reporting Service 186
Report IP Service 187
Link Me (IO) 192
VizIP DVR IP Alarm Integration 194
BACnet Service 195
Telephone Numbers 196
Sequential Dialing Attempts 198
Alternate Dialing Attempts 199

Advanced 201

Network Offline Module View 201
Network Online Module View 202
Network Module Reload 202
Network Init and Reboot 202
Module Network Statistics 203
Offline User Update 204
Network Security 204
Cancel Module Update 205
Reset Network Statistics 205
Testing Functions 205
Viewing Zones 205
Viewing Trouble Zones 206
Controlling PGM Outputs 207
Viewing Door Status 207
Profile Configuration 208
Changing Profiles 208
Programmable Function Configuration 209
Logic Control Function 211
Area Control Function 214
RTHP Control Function 217
Floor Tempering Control Function 225
Value Compare Function 230
Ripple Control PGM Output Function 232
Door Control Function 235
Virtual Door Function 238
Zone Follows PGM Function 241
Elevator Control 242
Register Counter 245

Output Compare 248

General Programming 250

Automation 250
Panel Configuration 253
System Controller Restart 260
System Controller Restart in Bios Mode 260
Custom Reader Format 261
Auto-addressing 264

View 266

View and Control Menu 266
Alarm Memory View 266
System Trouble View 267
Bypassed Zone(s) View 268
Viewing Door Status 268
Viewing Elevator Floor Status 269
Viewing Automation Status 270

Time 271

Set Time 271
Schedules 272
Holidays 276
Daylight Saving Adjustment 277

Bypass 279

Bypass Menu 279
Bypassing Zones 279
Bypassing Trouble Zones 279

System 281

System Menu 281
Answer Incoming Call 281
Call Remote Host 281
Send Test Zone 281

Reporting Tables 282

Contact ID Standard Zones 282
Contact ID Standard Trouble Zones 285
Contact ID Large Zones 289
Contact ID Large Trouble Zones 292
SIA Level 2 Standard Zones 296

SIA Level 2 Standard Trouble Zones 299
DVAC Surgard Zone 303
DVAC Surgard Trouble Zones 306

Reporting Codes 310

Area Reporting Codes 310
Custom Reporting Codes 310
CID (Contact ID) 310
SIA L2 (SIA Level Two) 311
DVAC (Surgard) 312
ModBUS Remote 312

Trouble Zone Maps 313

Control Panel 313
LCD Keypad 314
Zone Expander 314
PGM Expander 315
Reader Expander 315
Analog Expander 316

Profiles 317

Standard Profile 317
Access Control Profile 318
Elevator System Profile 320
School Profile 322
Storage Profile 323
Automation Profile 325
Apartment Profile 326

Data Register Definitions 329

Read/Write Memory Registers 329

Object Notation 330

Notation Structure 330
Module Object Type 330
System Object Type 330

Data Entry 333

Decimal Data Entry 333
Name and Text Data Entry 333
Access Code and PIN Number Entry 334
Date and Time Data Entry 334

Hexadecimal Data Entry 335
List Data Entry 335
Option Select Entry 336
PGM and PGM Group Entry 336
Zone Entry 337

Conversion 338

Hexadecimal Conversion 338
ASCII Conversion 340

Contact 342

Protege System

Introduction

This manual provides detailed references and programming examples to obtain optimal performance from your Protege System and the Protege System Management Suite. It covers the management of users, access levels, event reporting, and apartment complex and condominium systems.

This manual requires that the operator has an intermediate working knowledge of the Microsoft Windows operating system. Details of basic Windows functionality are beyond the scope of this document. For information about Windows, refer to the separate Windows user documentation.

System Controller

The Protege Integrated System Controller is the central processing system that runs the Protege System and makes nearly all decisions in the system. Designed using leading edge technology and high speed 32 Bit microprocessors the Protege System Controller is the ultimate in integrated solutions.

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 Module Network. Up to 250 modules can be connected to the Protege System in any combination to the network up to a distance of 900M (3000ft). Communication beyond this distance requires the use of a RS-485 Network Extender or slave communication extension with the PRT-RDI2/ PRT-RDE2 Protege Reader and Ethernet Reader Modules.

Locking a network prevents the removal, substitution or addition of modules to the module network effectively preventing any tampering with the system.

Features

- Up to 250 Areas
- Up to 2000 Zone Inputs
- Up to 1000 PGM Outputs
- Integrated Alarm, Access and Building Automation
- Multiple Integration Platforms, C-BUS, ModBUS, AMX and Serial Interface
- 2000 to 10000 users with no memory changes or adjustments
- Modular Communication and System Design
- Secure Encrypted RS-485 Module Communications
- Condominium and Apartment Functionality
- Industrial Automation Control and Logic
- Analog Input and Analog Output Interface
- C-Bus Home Automation Control (Dual Path Communications)

Protege System Management Suite

The Protege System Management Suite is a windows based professional integrated access control and alarm management system designed for any configuration from single site, single controller applications up to the global multi-national corporations using multiple site, multiple controller installations.

The Protege System Management Suite application is ideal for the configuration and management of your Protege installation. Special built in features and the quick-start kit will get your system up and running in minutes.

Protege Modules

The Protege System can be expanded to accommodate large numbers of modules using the encrypted RS-485 network. Modules that are currently available are listed below. Visit the Integrated Control Technology website (http://www.incontrol.co.nz) for the latest Protege module and product information.

Firmware Versions

The Protege System is a high performance integrated system and to ensure your installations are running at the optimal performance, we recommend that you utilize the latest firmware releases.

Product Code	Description	Version
PRT-CTRL	Protege System Controller	2.28.3106
PRT-KLCD	Protege LCD User Station	1.40.184
PRT-ZX16	Protege 16 Zone Input Expander	1.37.462
PRT-PX16	Protege 16 PGM Output Expander	1.33.153
PRT-ZXS16	Protege Standard 16 Zone Input Expander	1.35.93
PRT-PXS16	Protege Standard 16 PGM Output Expander	1.31.78
PRT-RDM2	Protege Mini 2 Reader Expander	1.48.216
PRT-RDS2	Protege Standard 2 Reader Expander	1.45.655
PRT-RDI2	Protege Intelligent 2 Reader Expander	1.64.1164
PRT-ADC4	Protege 4 Channel Analog Input Expander	1.30.55
PRT-DAC4	Protege 4 Channel Analog Output Expander	1.30.55

Firmware updates are available online from the ICT website (http://www.incontrol.co.nz) or through your distribution channel. If you are having difficulty downloading any firmware or finding the appropriate version please contact the ICT support team (mailto:support@incontrol.co.nz).

Menu Tree

Menu Reference

General operation and programming of the Protege Access and Alarm Management Controller requires the use of the menus on the keypad. The menu tree provides a reference guide to the menu options and the shortcuts to access them. A copy of the following pages and the options section can be used for a quick reference manual ideal for on site programming and maintenance.

Menu Tree

The Protege menu structure provides a simple and efficient method to access the programmable options within the Protege Controller. The menu can be accessed using shortcut keys for example to access the floor groups menu you could press [MENU, 2, 5]. Alternatively you can use the [↑] and [↓] keys to navigate through the menu tree and then press [ENTER] to make a selection.

```
*Main Menu*
1. Arm/Disarm
```

1. Arm/Disarm

```
*Main Menu*
2. Users
```

2. Users

1. Users
2. Menu Groups
3. Area Groups
4. Door Groups
5. Floor Groups
6. Access Levels

```
*Main Menu*
3. Events
```

3. Events

```
*Main Menu*
4. Installer
```

4. Installer

1. Modules
    1. LCD Keypad
    2. Zone Expander
    3. PGM Expander
    4. Reader Expander
2. Zones
    1. Zones

2. Trouble Zones
3. Zone Type

3. PGMs
4. Areas
5. Access
    1. Door
    2. Door Types
6. Groups
    1. PGM Group
    2. Keypad Group
7. Reporting
    1. Services
    2. Phone No
8. Advanced
    1. Network
    2. Testing
    3. Profiles
    4. Functions
9. General
    1. Automation
    2. Panel
    3. Restart

```
*Main Menu*
5. View
```

5. View

1. Alarm Memory
2. Trouble View
3. Bypass List
4. Door View
5. Elevator Floor
6. Automation

```
*Main Menu*
6. Time
```

6. Time

1. Change Time
2. Schedules
3. Holiday
4. Daylight

```
*Main Menu*
7. Bypass
```

7. Bypass

1. Zone
2. Trouble Zone

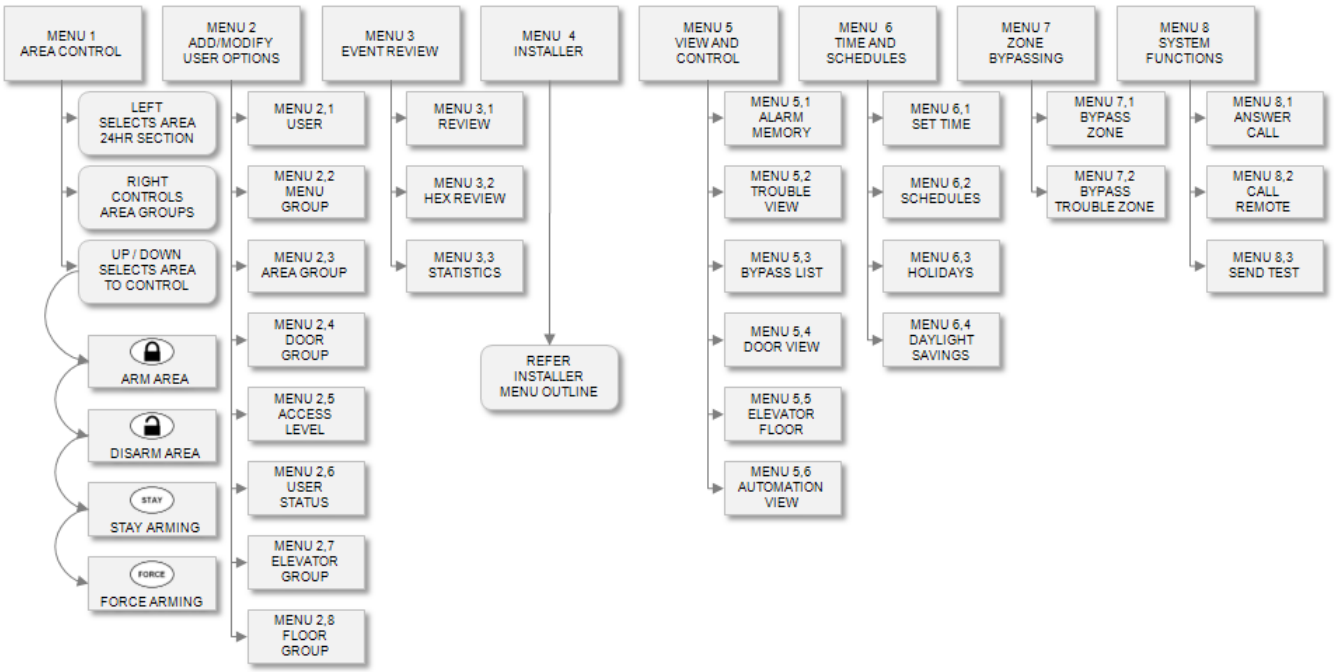
```
*Main Menu*
8. System
```

8. System

1. Answer Call
2. Call Remote
3. Test Report

Main Menu Chart

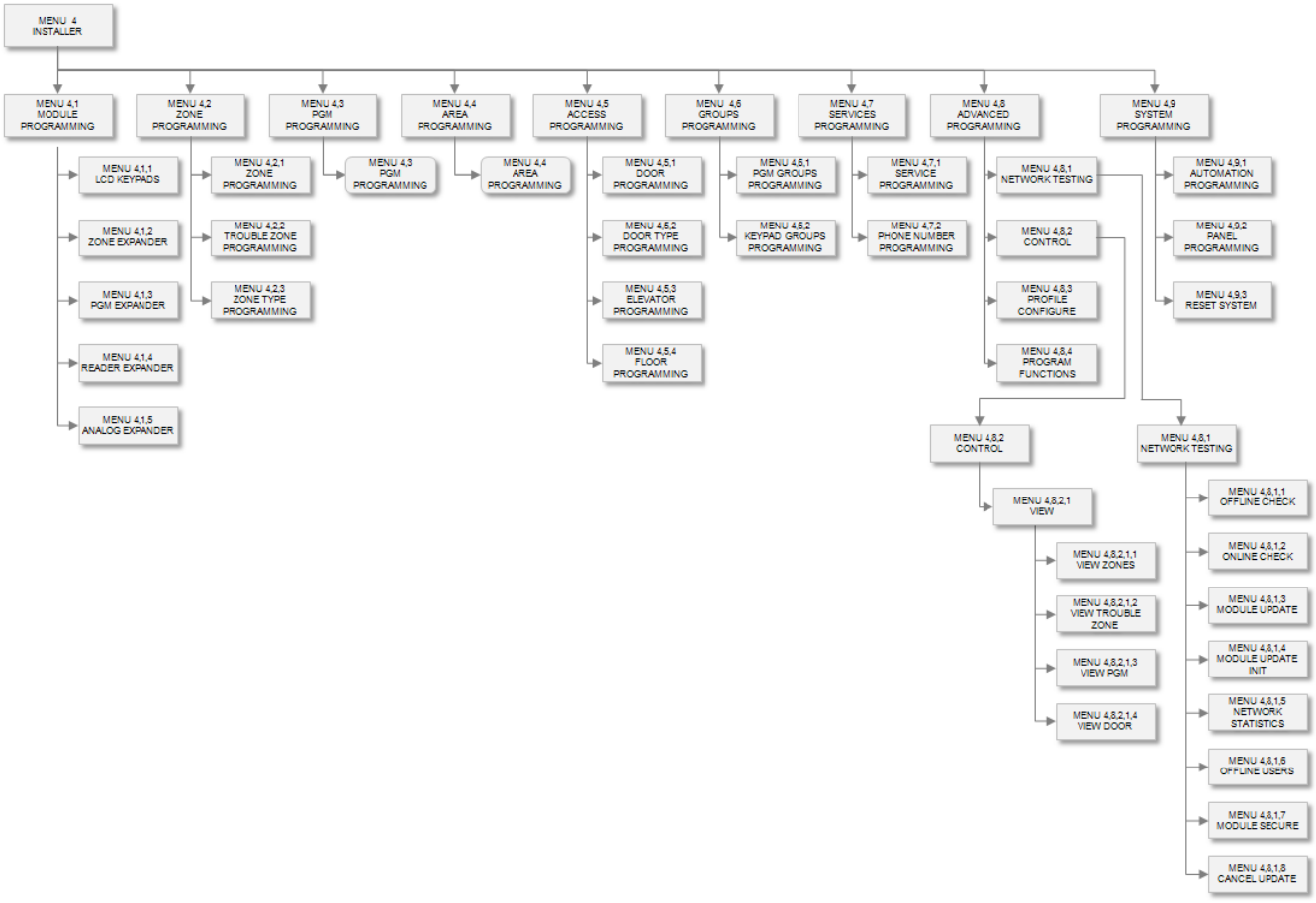
The Protege menu structure can also be shown as a menu chart with the sub menus under each of the main menu items. The chart is split in to the main menu and the installer menu.



Some menu options are not available to certain users. For example if you have logged in to the system as the Master User (UN00001, Default code 123456) then you will not have access to MENU, 4 (Installer). If you have logged in with the Installer User (UN00002, Default 000000) then you will not have access to MENU 1 (Area Control) or MENU 2 (Users). This can easily be changed by modifying the appropriate menu groups.

Installer Menu Chart

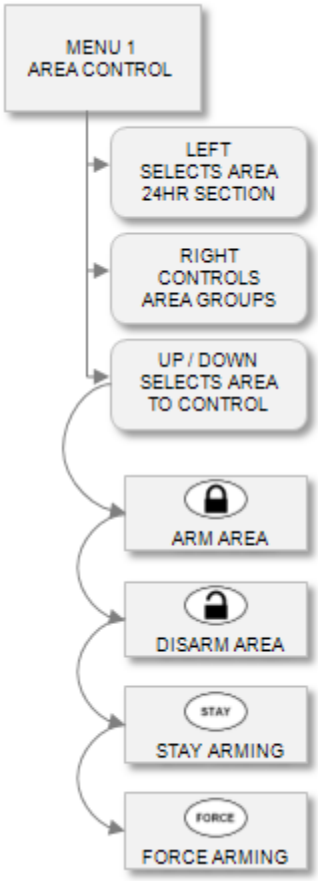
The Protege installer menu is available to the installer or any user who has the appropriate menu option programmed for their group.



The installer by default has access to the installer menu group. This can be programmed easily through menu groups. Multiple Installers can be programmed in the system.

Area Control

Area control allows you to arm/disarm areas/partitions in the Protege system. The area control provides access to group and 24HR arming options per area/partition.



Area Status Display

The area status display is a scrollable display showing the status of all the areas that the currently logged in user has access to. The screen only shows a single area at a time. Accessing the area status screen allows you to control that area for arming and disarming. The ability to limit the area's that a user has access to and which area's are displayed is programmable refer to the access level programming section.

```
*Area 001
is DISARMED
```

The area status display can be accessed in three ways depending on the programmed options for the user who logged in to the system and the configured options set for the keypad the user used to login.

- If *Direct Menu Mode* is turned on the user is taken directly to the Arm/Disarm menu item (first item available in the main menu) at which point they can select [MENU, 1].

  Shortcut Keys: [123456, ENTER, MENU, 1]
  Change Area Display: [↑] and [↓]

- If menu mode is tuned off the user will be taken directly to the area status display once they have logged in, this is a shortcut access and is recommended for most users. This is the default operation of the users with the exclusion of the installer.

  Shortcut Keys: [123456, ENTER]
  Change Area Display: [↑] and [↓]

- If the user is already logged in to the system the area status display can be access by selecting [MENU, 1].

Shortcut Keys: [MENU, 1]
Change Area Display: [↑] and [↓]

The area control functions allow the user to perform the following actions on the selected area.

- Disarming (see page 18)
- Regular Arming (see page 16)
- Force Arming (see page 17)
- Stay Arming (see page 17)
- 24HR Enabling (see page 18)
- 24HR Disabling (see page 19)
- Area Group Arming (see page 19)
- Area Group Disarming (see page 20)

Area Security

The area status display does not show all areas to all users. The area security control with the Protege allows various groups of area's to be displayed to a user depending on the access that the user has and the area's that are allowed to be controlled by the keypad they have logged in to.

- The keypad that the user has logged in to will display the primary area that is assigned to that keypad if the user who logged in has access to the primary area.
- If the area is disarmed, it will be displayed if the area belongs to the keypad group and to either the user arm group or disarm group.
- If the area is armed, it will be displayed if the area belongs to the keypad group and the disarm group.

By default all keypads have access to all areas and the ability for a person to control an area is processed by their arm/disarm groups assigned to their access level. By default if an area is assigned to the disarm group of a user they will also have access to arm that area.

Regular Arming

Regular arming arms your area using a standard or regular arming process and will arm all zones within the selected area. The selected area can only be armed if it is in the "disarmed" state and all zones are closed. To arm the selected area, you must be able to access it, refer to the Area Security section (see page 16).

- Access the area status display screen as explained in section Area Status Display (see page 15). Using the scroll keys [↑ ↓] select the area that you want to control.

```
*Area 001
is DISARMED
```

- From the Area Status Display screen, press the [ARM] key to regular arm the area. Pressing the [ARM] key starts the exit delay, if programmed. It enables all the zones assigned to the area and checks that they are ready to be armed. The area's status will then change showing each step in the regular arming process. When the area is armed the area status will change to the ARMED state. If an exit delay is programmed the area will enter the exit delay cycle. Refer to the Arming Failure section (see page 20) for messages during the arming process or if the area cannot arm.
- Press the [DISARM] key at any time during the arming process to abort the arming process and return the area to the DISARMED state.
- Press the Clear key to exit.

The area status display can be programmed to display only selected area's to certain users. The area security control with the Protege allows specific groups of area's to be displayed to a user, refer to the Area Security section (see page 16). Refer to the Access Levels Section (see page 39) for information on how to set and program area groups in access levels.

Force Arming

Force arming allows you to quickly arm your system even though zones are open. The open zones are then ignored by the system while the arming process takes place. If an open zone closes after the area is armed, the zone is no longer ignored by the system and the area will generate an alarm if the zone is opened again. The area can only be force armed if its status is "disarmed" and if it the open zones have the Force Arming option turned on.

- Access the area status display screen as explained in the section Area Status Display (see page 15). Using the scroll keys [↑ ↓] select the area that you want to force arm.

  ```
  *Area 001
  is DISARMED
  ```

- From the Area Status screen, press the [FORCE] key to force arm an area. Pressing the [FORCE] key starts the exit delay, if programmed. It checks all zones assigned to the area are sealed and any zone that is open with the forced arm option enabled in the assigned zone type. If zone(s) do not have a zone type that has the force arm option enabled it checks that they are ready to be armed.
- When completed the zone testing procedure the areas status will change "force armed".

  ```
  *Area 001
  is FORCE ARMED
  ```

- Pressing the [DISARM] key at any time during the force arming process will abort the force arming process and return the area to the disarmed state. Press the [CLEAR] key to exit.

To force arm the selected area, you must be able to access it, refer to the Area Security section (see page 16). Refer to the Arming Failure section (see page 20) if the area cannot arm or displays an error message when attempting to force arm the selected area.

Stay Arming

Stay arming partially arms your area to permit you to remain in your home or office by arming the outer (perimeter) zones of the protected area (i.e. doors and windows). The area can only be stay armed if its status is "disarmed" and if it contains zones whose Stay Zone option is turned on.

- Access the area status display screen as explained in section Area Status Display (see page 15). Using the scroll keys [↑ ↓] select the area that you want to stay arm.

  ```
  *Area 001
  is DISARMED
  ```

- From the Area Status screen, press the [STAY] key to stay arm an area. Pressing the [STAY] key starts the exit delay, if programmed. It enables all the stay zones assigned to the area and checks that they are ready to be armed.
- When completed the zone testing procedure the areas status will change "stay armed".

  ```
  *Area 001
  is STAY ARMED
  ```

- Pressing the [DISARM] key at any time during the stay arming process will abort the stay arming process and return the area to the disarmed state. Press the [CLEAR] key to exit.

To stay arm the selected area, you must be able to access it, refer to the Area Security section (see page 16). Refer to the Arming Failure section (see page 20) if the area cannot arm or displays an error message when attempting to force arm the selected area.

Disarming

The area can be disarmed if it is armed in any of the possible arming states explained in the previous sections. For information on disarming an area using a card access reader or other special function refer to the Protege Programming Manual.

- Access the area status display screen as explained in section Area Status Display (see page 15). Using the scroll keys [↑ ↓] select the area that you want to disarm.
- From the Area Status screen, press the [DISARM] key to disarm the selected area. Pressing the [DISARM] key starts the disarming process.
- When the disarming process is completed the area status will change to "disarmed".

```
*Area 001
is DISARMED
```

- Press the [CLEAR] key to exit.

To disarm the selected area, you must be able to access it, refer to the Area Security section (see page 16).

24HR Enabling

The Protege System continually checks zones and trouble zones for a tamper condition regardless of the armed status of the area. The 24Hr processing monitors trouble zones as well as tamper and shorts on zones within the selected area. This allows the tamper zones to generate an alarm even if the area is disarmed. To enable the 24Hr processing of an area, you must have access to the area and the user must have the option to access the 24Hr Processing enabled.

- Access the area status display screen as explained in section Area Status Display (see page 15) . Using the scroll keys [↑ ↓] select the area that you want to disarm.

```
*Area 001
is DISARMED
```

- From the Area Status screen, press the [←] key to select the 24Hr Status screen.

```
*Area 001
24HR Disabled
```

- From the Area 24Hr Status screen, press the [ARM] key to arm/enable the 24Hr processing in the selected area. Pressing the [ARM] key starts the 24Hr enable/arming process.

```
*Area 001
24HR Busy
```

- When the enable/arming process is completed the 24Hr area status will change to "24Hr Enabled".

```
*Area 001
is ENABLED
```

- Press the [➔] key to return to the area status display.
- Press the [CLEAR] key to exit.

To enable the 24Hr processing of the selected area, you must be able to access it, refer to the Area Security (see page 16). The user must have the access 24Hr Processing Option enabled.

The Protege System protects the area programming by preventing ANY programming to be done when either the Area or the 24Hr processing of an area is enabled. You must always disable the 24Hr processing and disarm an area before the area can be programmed.

24HR Disabling

The Protege System continually checks zones and trouble zones for a tamper condition regardless of the armed status of the area. The 24Hr processing monitors trouble zones as well as tamper and shorts on zones within the selected area. This allows the tamper zones to generate an alarm even if the area is disarmed. To disable the 24Hr processing of an area, you must have access to the area and the user must have the option to access the 24Hr Processing enabled.

- Access the area status display screen as explained in section Area Status Display (see page 15). Using the scroll keys [↑ ↓] select the area that you want to disarm.

  ```
  *Area 001
  is DISARMED
  ```

- From the Area Status screen, press the [←] key to select the 24Hr Status screen.

  ```
  *Area 001
  24HR Enabled
  ```

- From the Area 24Hr Status screen, press the [DISARM] key to disarm/disable the 24Hr processing in the selected area. Pressing the [DISARM] key starts the disable/disarming process.

  ```
  *Area 001
  24HR Busy
  ```

- When the 24Hr disable/disarming process is completed the 24Hr area status will change to "24Hr Disabled".

  ```
  *Area 001
  24HR Disabled
  ```

- Press the [→] key to return to the area status display.
- Press the [CLEAR] key to exit.

To disarm the 24Hr processing of the selected area, you must be able to access it, refer to the Area Security (see page 16). The user must have the access 24Hr Processing Option enabled.

The Protege System protects the area programming by preventing ANY programming to be done when either the Area or the 24Hr processing of an area is enabled. You must always disable the 24Hr processing and disarm an area before the area can be programmed.

Area Group Arming

Area group processing allows you to arm or disarm a group of areas rather than one area at a time. The area group controlled is the area group assigned to the keypad used to access the system. To arm the area group the user must be able to access ALL the areas in the area group. The user must have the access area group option enabled to access the area group function.

- Access the area status display screen as explained in section Area Status Display (see page 15).

  ```
  *Area 001
  is DISARMED
  ```

- From the Area Status screen, press the [→] key to select the Area group control screen.

  ```
  Press [ARM] or
  [DISARM] to
  ```

  The screen will scroll between the screen above and below prompting the user to press the [ARM] or [DISARM] key to control the area group that is shown.

  ```
  control group
  *Area Group 001
  ```

- From the Area Group Control screen, press the [ARM] key to arm the selected area group. Pressing the [ARM] key starts the arming process for each area in the area group.
- When the area group arming process is completed the display will return to the area group control screen.
- Press the [←] key to return to the area status display.
- Press the [CLEAR] key to exit or the [MENU] key to select another menu option or function.

Area Group Disarming

Area group processing allows you to arm or disarm a group of areas rather than one area at a time. The area group controlled is the area group assigned to the keypad used to access the system. To disarm the area group the user must be able to access ALL the areas in the area group. The user must have the access area group option enabled to access the area group function.

- Access the area status display screen as explained in section Area Status Display (see page 15).

  ```
  *Area 001
  is DISARMED
  ```

- From the Area Status screen, press the [➔] key to select the Area group control screen.

  ```
  Press [ARM] or
  [DISARM] to
  ```

  The screen will scroll between the screen above and below prompting the user to press the [ARM] or [DISARM] key to control the area group that is shown.

  ```
  control group
  *Area Group 001
  ```

- From the Area Group Control screen, press the [DISARM] key to disarm the selected area group. Pressing the [DISARM] key starts the disarming process for each area in the area group.
- When the area group disarming process is completed the display will return to the area group control screen.
- Press the [🡐] key to return to the area status display.
- Press the [CLEAR] key to exit or the [MENU] key to select another menu option or function.

Arming Failure

There are a number of reasons why an area might fail to arm, such as zones within the area that remain open, or a trouble condition within the system. The different arming failures and possible user actions are described in the following sections.

Zone(s) Open Display

```
*CP001:01
is OPEN
```

- If a zone is not closed and secure, the keypad immediately beeps and displays the first open zone.

  ```
  Press [ARM] to
  Re-test zone(s)
  ```

  The keypad then automatically scrolls through the different possible actions that the user is allowed to take to continue with the arming process.

  ```
  Press [🡓] for
  next zone(s)
  ```

- Press the [ARM] key to retest all the zones. Any exit zone with the exit delay or delay zone type programmed will not prevent the system from arming if the *Exit Zone* option is enabled. A bypassed zone will not prevent the system from arming unless the number of bypassed zone(s) exceeds the maximum number allowed for the selected area. To program a maximum number bypassed zones that an area can have refer to the Bypass Count option in Area Programming (see page 114).

  ```
  Press [FORCE] to
  force arm area.
  ```

- Press the [🡓] key, to scroll through the zones that remain open when arming the area.

  ```
  Press [MENU, 7]
  to bypass zones.
  ```

  If the zone is still open and the area disarmed, you can force the area to arm. Press the [FORCE] key to force arm the area. Force arming must be enabled for the area being controlled and the user must have access to this operation. Refer to the Force Arming section (see page 17) for more information.

- Press [MENU, 7] to access the bypass menu. Accessing the bypass menu allows you to bypass zones and trouble zones. Refer to the section Bypassing Zones (see page 279) for more information.

System Trouble

When arming the system, if a general, system or access trouble is present, the keypad momentarily displays a trouble message and returns to the Area Status screen.

```
Cannot ARM Area
System Trouble
```

To prevent an area from arming when a trouble condition occurs, the No Arming On Trouble Condition option must be turned on. For a description of the trouble conditions refer to the Trouble Group Table (see page 96).

Area Busy

If the area is busy, either another user is arming or disarming the area at the same time or the system is busy completing a task that cannot be interrupted by a user action.

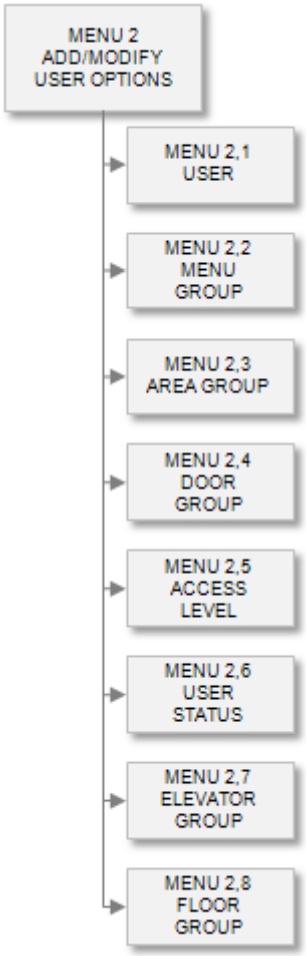
```
Area Busy
Please wait...
```

Try the action again a few seconds later. If the area is no longer busy, you can perform your action that you requested.

It is always good practice to verify that the area has not changed status because of a system or user controlling the selected area.

Users

To access the user programming menu, login using the valid master code and then select [MENU, 2]. You will then have a menu of user functions that you can program in the Protege System. Users have access levels that are assigned to them for the purpose of controlling what the user or group of users have access to within the Protege System. Access levels will have Schedules, Door Groups, Area Groups and Menu Groups assigned. This method of assignment allows flexible method of user control.



The system comes pre-programmed with 3 default users, Master, Installer and Demo User. It is recommended that the default settings of these users such as the access level and the settings in their respective access levels not be modified.

It is recommended to change the Master and Installer login codes to protect your system from unlawful access.

Caution is required when modifying users, menu groups, door groups, area groups and access levels. Changing the master and installer menu items can lock out these special users from the system. To gain access you will need to default the system.

User Programming

To access the user programming login using a valid master code and then select [MENU, 2, 1]. The screen displays "Select user to modify" as shown in the following example.

```
Select user to
modify: UN00001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the users in the Protege allow you to configure how user will interact with the system and the options each user will have.

When programming a user that will require the loiter feature to be enabled the users expiry time will be reduced to a date only and you will not be able to set a time for the user. The time is used to control the loiter time that this user will be allocated in the loiter areas.

Selecting a User to Modify

Each user is assigned a unique user number from 00001 to 65535. When selecting a user to modify the user number who logged in to the keypad will be shown.

```
Select user to
modify: UN00001
```

Type the appropriate 5-digit user number or use the [🡻] and [🡹] keys to scroll the available user numbers. When the desired user number appears on the screen, press [ENTER] to program the selected user number. The maximum number of users that can be programmed is limited by your system's memory and configured profile.

User Names

If the selected user has a name associated (some users do not have a name associated with them) the name programming screen will be shown.

```
UN00001 Name
Master
```

To scroll users by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected user use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the user name will be prefixed by an '*' this indicates that the name is an editable name in the system. Some users do not have names, this is limited by the system memory and the profile configured.

User Access Code or PIN Number

The user code (PIN) can be from 1 to 8 digits in length. Entering a user code (PIN) that already exists in the system results in the system generating an error and alerting the owner of that code. To modify or enter a new pin number for the selected user follow the instructions in the section Entering PIN Numbers (see page 334) and press [ENTER].

```
UN00001 Enter
code: 123456
```

For users to modify their own code or the code of another user with the same access level, the appropriate code modification options must be turned refer to User Special Options (see page 29).

Access Level Assignment

The access level determines what rights this user will have in the Protege system. For more information on the programming of the access level refer to the Access Level Programming section (see page 39). Each user can be assigned four different access levels, when a user requests a certain action the Protege system checks each of the access levels in order until it finds one that has rights to perform the requested action. Each access level can also be assigned an independent start and end time.

```
UN00001 Access
*Access Lvl 001
```

Use the [1] and [3] keys to scroll the access level selection and press [ENTER] to select the access level displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335) .

Access Level 1 Start Date

Setting the access level start date will disable the access level for this user until 00:00 on this date. If a start time is also set the access level will be disabled until that time has past on this date.

```
UN00001 Axs1 Sta
date: --/--/----
```

Use the numerical keys to enter a valid date and then press [ENTER] to program the date. If you do not program a time in the following section the access level will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334).

If you do not enter a valid date an error message will be shown, pressing the [STAY] key will allow you to clear your entry or set the default value.

Access Level 1 Start Time

Setting the access level start time will disable the access level for the user until this time has past. If both the start time and date are set then the access level will remain disabled until the date and time has past. If only the time is set then the access level will be disabled until this time has past and will then remain enabled until either the access level end time expires or until the midnight of that day.

Use this feature to program cards for temporary employees, trade people or contractors. This feature can also be used for membership processing to prevent access once the membership period has expired.

```
UN00001 Axs1 Sta
time: --:--
```

Use the numerical keys to enter a valid time in a 24HR format and then press [ENTER] to program the time. If you do not program a time in the following section the user will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334) .

If you do not enter a valid time an error message will be shown, pressing the [STAY] key will allow you to clear your entry.

Access Level 1 End Date

Setting the access level end date will disable the access level for this user at 23:59 on this date. If a end time is also set the access level will be disabled at that time on this date.

```
UN00001 Axs1 End
date: --/--/----
```

Use the numerical keys to enter a valid date and then press [ENTER] to program the date. If you do not program a time in the following section the access level will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334).

If you do not enter a valid date an error message will be shown, pressing the [STAY] key will allow you to clear your entry or set the default value.

Access Level 1 End Time

Setting the access level end time will disable the access level for the user once this time has past. If both the end time and date are set then the access level will be disabled after the date and time has past. If only the time is set then the access level will be disabled after this time has past.

```
UN00001 Axs1 End
time: --:--
```

Use the numerical keys to enter a valid time in a 24HR format and then press [ENTER] to program the time. If you do not program a time in the following section the user will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334).

If you do not enter a valid time an error message will be shown, pressing the [STAY] key will allow you to clear your entry.

Access Level 2,3 and 4

Each user can be assigned up to four access levels. Each of these access levels has an independent start and end time. These are programmed after Access Level 1. Leave the access level as None to disable it.

User Area

The user area can be used to disarm the selected area automatically on login to a keypad or when access is granted at a door or reader. For this feature to operate correctly the programmed area must belong to the user's disarm area group. This feature is ideal for securing many individual offices yet arming all of them when all employees exit and disarming only the person's office that they are allowed to access while other offices remain secure and protected.

```
UN00001 Area
None
```

Use the [1] and [3] keys to scroll the user area selection and press [ENTER] to select the area that is displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

User Expiry Date

Setting an expiry date for the user will prevent the user from gaining access to the system past the date that is set. Use this feature to program cards for temporary employees, trade people or contractors. This feature can also be used for membership processing to prevent access once the membership period has expired.

```
UN00001 Expiry
date: --/--/----
```

Use the numerical keys to enter a valid date and then press [ENTER] to program the date. If you do not program a time in the following section the user will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334).

If you do not enter a valid date an error message will be shown, pressing the [STAY] key will allow you to clear your entry or set the default value.

User Expiry Time

Setting an expiry time for the user will prevent the user from gaining access to the system past the date and time that is set. If you have created a temporary user by programming the expiry date in the previous screen, use the 24-hour clock method (i.e. 4:15pm = 16:15) to program the time that the user code (PIN) and its programmed rights become invalid. If the expiry date in the previous screen is left blank, the system ignores the time.

If the time screen is left blank, but an expiry date has been programmed, the user code (PIN) expires at 23:59.59 on the date programmed.

If the *Loiter Mode* option is turned on for this user, the expiry time is ignored and the user code (PIN) expires at 23:59.59 on the programmed date.

Use this feature to program cards for temporary employees, trade people or contractors. This feature can also be used for membership processing to prevent access once the membership period has expired.

```
UN00001 Expiry
time: --:--
```

Use the numerical keys to enter a valid time in a 24HR format and then press [ENTER] to program the time. If you do not program a time in the following section the user will expire at midnight on the date that is programmed. For more information about entering the date information refer to the section Date and Time Data Entry (see page 334).

If you do not enter a valid time an error message will be shown, pressing the [STAY] key will allow you to clear your entry.

User Family / Facility Number

When a user requires control of card readers and access functions in the Protege System they must be programmed with a facility code or family number and a card number. The first screen shown will be the family number of the access control card that will be given to the user, enter the family number of the card and then press [ENTER].

```
UN00001 Facility
id: 4294967295
```

The family number is not normally printed on the card or tag. This is typically provided on a reference document provided with the cards at the time they are purchased. If you are not sure of the facility code or card number you can present the card to any reader that is programmed in the system. The facility or family id number that is read will be displayed in the screen only if it is not already programmed or allocated to a user.

The number 4294967295 is the maximum facility code and is a reserved number, setting this number will disable the card for this user.

User Card Number

When user requires control of card reader and access functions in the Protege System they must be programmed with a card number. Type the family or facility code in the previous entry and the card number of the access control card that will be given to the user in the card number entry below then press [ENTER].

```
UN00001 Card
no: 4294967295
```

The card number when blank or deleted is shown as the maximum card number of 4294967295 and to default or clear the card number press the [DISARM] key.

If you are not aware of the card number you can present the card to any reader that is programmed in the system. The card number that is read will be displayed in the location only if it is not already programmed or allocated to a user.

The Protege System also supports the loading of cards automatically. This will increment the user number and wait for the next valid presentation of a card that is not currently in the database and storing the details for that user in the current record.

- To enable automatic loading of the card information press the [ARM] key and a brief message will be shown with the current automatic card loading status.

  ```
  Autoload mode
  enabled.
  ```

- Once the screen returns to the facility id entry screen as shown below presenting a card to a reader will program the card in to the system and automatically increment the user number. The facility and the card number will be programmed when the auto loading is enabled.

  ```
  UN00001 Facility
  id: 4294967295
  ```

- To disable the automatic card loading mode press the [ARM] key which will toggle the automatic card loading mode back to disabled.

  ```
  Autoload mode
  disabled.
  ```

User Secondary Family / Facility Number

Each user can be assigned two separate cards. To program a second card enter the family number of the card and then press [ENTER].

```
UN00001 2nd Fac
id: 4294967295
```

The number 4294967295 is the maximum facility code and is a reserved number, setting this number will disable the card for this user.

User Secondary Card Number

Each user can be assigned two separate cards. To program a second card enter the family number of the card and then press [ENTER].

```
UN00001 2nd Card
no: 4294967295
```

The card number when blank or deleted is shown as the maximum card number of 4294967295 and to default or clear the card number press the [DISARM] key.

User Language

Each User can be programmed with a default language that will be loaded by the System Controller when they log into a keypad.

```
UN00001 Language
None
```

If no language is selected the default panel language will be displayed.

User Miscellaneous Options

Options that relate to general functions of the user can be set using option entry.

```
UN00001 Misc
   [1-34----]
```

To modify options, use the follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 - Greeting Mode

- Enabled the user will be presented on the keypad screen with a time of day greeting when they log in to the keypad. For example "Good Morning Mr. Smith" or "Good Afternoon Mr. Jones".
- Disabled the user will not be shown a greeting when they log in to the keypad.

This option when enabled can be overridden by the same option in the menu group. To control this option per individual user disable the option in the menu group and assign this option for each user that requires a greeting message displayed on login.

Option 2 - Menu Mode

- Enabled the user will be taken directly to the menu. Normally a user will be shown the status of the current area that the keypad belongs to however this feature allows users that can not perform any area commands or that are more likely to perform menu commands to be taken directly to the menu without pressing the [MENU] key when they log in.
- Disabled the user will be taken to the primary area status screen if they have access to the programmed area.

Option 3 - Alarm Acknowledgement Allowed

- Enabled the user can acknowledge and delete alarms that are stored in memory for an area by using the [ENTER] key. To acknowledge alarms, the user must have access to the View menu. The area where the alarm occurred must also belong to the user's disarm area group.
- Disabled the user will not be able to acknowledge alarms.

This option when enabled can be overridden by the same option in the menu group. To control this option per individual user disable the option in the menu group and assign this option for each user.

Option 4 - Show Alarm Memory On Login

- Enabled the user when logging in to the keypad will be displayed any existing alarm for the keypad's primary area. If an alarm occurred in any other area, the alarm memory is sent to the alarm buffer, which can be viewed through the View menu. To view the alarm memory, the user must be allowed to access the View menu. The keypad's primary area must also belong to the user's disarm area group. If you want to acknowledge the alarm, the Alarm Acknowledgment option must be turned on.
- Disabled the keypad will take no action if alarm memory is present when a user logs in.

This option when enabled can be overridden by the same option in the menu group. To control this option per individual user disable the option in the menu group and assign this option for each user.

Option 5 - Automatic Primary Area Disarm

- When enabled and the user logs in to the keypad, the primary area associated with the keypad automatically disarms. The keypad's primary area must belong to the user's disarm area group. This feature does not automatically cancel the arming process of an area that was previously started.
- Disabled the keypad will not perform any action when the user logs in.

Option 6 - User Area Disarm On Login

- When enabled on login, the area assigned to the user automatically disarms. The user area must belong to the user's disarm area group. This feature does not automatically cancel the arming process of an area.
- Disabled the keypad will not perform any action when the user logs in.

Option 7 - User Troubles Acknowledgment

- When enabled the user can acknowledge and clear user troubles that are stored in memory for an area by using the [ENTER] key when viewing these troubles in the View menu.

  For this option to operate correctly the user must have access to the View menu and the Trouble Acknowledgment option must be turned on.
- Disabled the user can not acknowledge user troubles.

Option 8 - System Troubles Acknowledgment

- When enabled the user can acknowledge and clear system troubles that are stored in memory for the entire system by using the [ENTER] key when viewing these troubles in the View menu.

  For this option to operate correctly the user must have access to the View menu and the Trouble Acknowledgment option must be turned on.
- Disabled the user can not acknowledge system troubles.

User Special Options

Options that relate to special functions of the user can be set using option entry.

```
UN00001 Special
   [1-34----]
```

To modify options, use the follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 – User Area is a Group

When this option is enabled the users area selection screen will change to a group selection allowing multiple areas to be controlled by the user area group configuration.

- Enabled the user area will be set as a group.
- Disabled the user area selection will be an individual area.

Option 2 - Reserved

- Reserved do not modify.

Option 3 - Super User Code

- Enabled the user is assigned a super user status that allows them to override dual code functions and anti-passback violations.
- Disabled the user does not have super user status.

Option 4 - User Can Modify Own Code

- Enabled the user will be able to modify their own code. The user must have access to the user menu. The user can not modify any access or other functions.
- Disabled the user can not modify their own code.

Option 5 - Reserved

- Reserved do not modify.

Option 6 - Loiter Mode User

- When enabled the user has access to any loiter area for a limited amount of time. If the loiter time has elapsed and the user did not exit the area, then the user cannot exit the area until a master user resets the user's loiter time.

  For this option to work the Loiter Mode option must be turned on for each area that requires this function. A loiter time and a loiter area must also be programmed. Furthermore, the area requires an entry and exit reader set with the anti-passback feature to control the user traffic.

  The loiter mode is ideal for use in car park control to prevent multi level car parks that have both tenant and Public car parks from being used by tenants.
- Disabled the user will not operate in a loiter mode when entering a area programmed with the loiter option.

Option 7 - Remote Login

- When enabled the user code and user number can be used for remote login through one of the many available services. For upload and download of information using the computer system at least one remote login user must be defined, this can be an active user in the system.
- Disabled the user cannot be used for remote login.

Option 8 - Duress User

- When enabled the user code will trigger the duress trouble zone for the keypad that the user logged in to.

  For this option to operate correctly the duress trouble zone must be programmed in to an area that is armed.
- Disabled the user is not a duress user.

Menu Groups

To access the menu group programming login using a valid master code and then select [MENU, 2, 2]. The screen displays "Menu group to modify" as shown in the following example.

```
Menu Group to
modify: MG001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the menu groups in the Protege allows you to configure how a user will interact with the keypads in the system.

Selecting a Menu Group to Modify

Each menu group is assigned a unique menu group number from 001 to 250.

```
Menu Group to
modify: MG001
```

Type the appropriate 3-digit menu group number or use the [🡻] and [🡹] keys to scroll the available menu groups. When the desired menu group appears on the screen, press [ENTER] to program the selected menu group number. The maximum number of menu groups that can be programmed is limited by your system's memory and configured profile.

Menu Group Name

If the selected menu group has a name associated (some menu groups do not have a name associated with them) the name programming screen will be shown.

```
MG001 Name
All Menus
```

To scroll menu groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected menu group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the menu group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the menu group determines when the menu group is valid and if it will use a secondary menu group if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
MG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Menu Group

A secondary menu group can be selected that will be used when the schedule of the menu group that is programmed is not valid. The schedule of the secondary menu group must be valid. The secondary group allows very powerful menu controls to be placed on users during certain times of the day.

```
MG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary menu group selection and press [ENTER] to select the menu group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary menu group that uses the current menu group being edited will perform no function.

Menu Group Main Menu Options

Options that relate to ability for this menu group to access the main menu (items 1 to 8).

```
MG001 Main
   [123-5678]
```

To modify options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 - Area Control Menu

- Enabled the menu group will allow a user access to the area control menu [MENU, 1].

  All users that are required to perform area control must have this option enabled for the menu group assigned to their access level.
- Disabled the menu group will not allow access to the area control menu.

Option 2 - User Menu

- Enabled the menu group will allow a user access to the user programming menu [MENU, 2].

For a menu group to also allow access to the programming of door groups, area groups, menu groups and access levels the user sub menu option must also be enabled.

- Disabled the menu group will not allow access to the user programming menu.

Option 3 - Event Review Menu

- Enabled the menu group will allow a user access to the event review menu [MENU, 3].
- Disabled the menu group will not allow access to the event review menu.

Option 4 - Installer Menu

- Enabled the menu group will allow a user access to the installer programming menu [MENU, 4]. All users that require to program modules and installation parameters must have this enabled for the menu group assigned to their access level.

  The installer menus also contain advanced sub menus and to access these menu items the advanced sub menu items must be turned on for the menu group assigned to the users access level.
- Disabled the menu group will not allow access to the installer programming menu.

Option 5 - View Menu

- When enabled the menu group will allow a user access to the status view menu [MENU, 5].

  The view menu will allow a menu group to access the alarm memory, bypass status and trouble status information for the system.
- Disabled the menu group will not allow access to the status view menu.

Option 6 - Time Menu

- When enabled the menu group will allow a user access to the time menu [MENU, 6]. This allows the programming of time related functions and the system time in the controller.

  If a user requires access to the programming of schedules and daylight saving configuration parameters the menu group must also have the time sub menu option enabled.
- Disabled the menu group will not allow access to the time menu.

Option 7 - Bypass Zone Menu

- When enabled the menu group will allow a user access to the bypass zone menu [MENU, 7]. This will allow a user access to zones that can be bypassed in the system.
- Disabled the menu group will not allow access to the bypass zone menu.

Option 8 - System Menu

- When enabled the menu group will allow a user access to the system menu [MENU, 8]. This will allow a user access to the system functions used to generate a test report, dial the remote computer that is programmed or answer an incoming call from the remote computer.
- Disabled the menu group will not allow access to the system menu.

Menu Group Sub Menu Options

Options that relate to ability for this menu group to access the sub menu items that relate to main menus that are selected including arming and special keypad control functions.

```
MG001 Sub
   [-2345678]
```

To modify options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 - Advanced Sub Menu

- Enabled the menu group will allow a user access to the advanced sub menus under the installer menu [MENU, 4, 8].

- This option will not operate unless the menu group also has the installer option enabled in the main menu options.
- Disabled the menu group will not allow access to the advanced sub menus.

Option 2 - Time Sub Menu

- Enabled the menu group will allow a user access to the time sub menus that allow configuration of schedules and daylight saving settings. The menu group must also have the main time menu option enabled.
- Disabled the menu group will not allow access to the user programming menu.

Option 3 - Bypass Trouble Zone Sub Menu

- Enabled the menu group will allow a user access to the bypass sub menu for the control of trouble zones [MENU, 7, 2]. The menu group must also have the bypass menu option enabled in the main menu options for this to operate correctly.
- Bypassing trouble zones is not recommended unless instructed by an installer.
- Disabled the menu group will not allow access to the trouble zone bypass sub menu.

Option 4 - Area Group Access

- Enabled the menu group will allow a user access to the area group control screen from the area status display screen. Refer to the Area Group Control Functions (see page 19) .
- Disabled the menu group will not allow access to the area group control screens.

Option 5 - 24HR Processing Access

- When enabled the menu group will allow a user access to the 24HR processing status screen and the control of the 24HR tamper section of an area. Refer to the 24HR Control Functions (see page 18).
- Disabled the menu group will not allow access to 24HR Processing and Control.

Option 6 - Stay Arming

- When enabled the menu group will allow a user to stay arm an area. The area must also have the stay arming option enabled.
- Disabled the menu group will not allow area stay arming.

Option 7 - Force Arming

- When enabled the menu group will allow a user to force arm an area. The area must also have the force arming option enabled.
- Disabled the menu group will not allow force arming.

Option 8 - Instant Arming

- When enabled the menu group will allow a user to instant arm an area. The area must also have the instant arming option enabled.
- Disabled the menu group will not allow instant arming.

Menu Group Extra 1 Menu Options

Options that control the access this menu group has to certain menus and functions.

```
MG001 Extra 1
   [1-------]
```

To modify options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 - User Sub Menu

- Enabled the menu group will allow a user access to the user sub menus under the user menu [MENU, 2]. This option will not operate unless the menu group also has the user menu option enabled in the main menu options.
- Disabled the menu group will not allow access to the user sub menus.

Option 2 - Installer Menu Group

- Enabled the menu group when assigned to a user and that user logs in to a keypad the Installer Login Trouble Zone will be opened. When they log out the installer trouble zone will be closed.
- Disabled the menu group will not change the installer login trouble zone.

When this option is enabled and assigned to a user who uses the menu group in their access level (by default the installer responsible for the system) the keypad logout time will be overridden and set to never log the user out. For more information refer LCD Keypad Programming.

Option 3 - Display User Greeting On Login

- Enabled the menu group will display the time of day greeting to the user once they have entered their user code.
- Disabled the display of the user login greeting.

This option is overridden by the display user greeting option that can be assigned to individual users.

Option 4 - Allow User Memory Acknowledge

- Enabled the user will be able to acknowledge alarm memory that is displayed when they first login.
- Disabled the user will not be able to acknowledge memory.

This option is overridden by the acknowledge memory option in the user programming if it is enabled.

Option 5 - Display Memory To User On Login

- Enabled the user will be shown any alarms that are in the memory when they log in to the keypad.
- Disabled the memory will not be shown.

This option is overridden by the display memory option in the user programming if it is enabled.

Option 6, 7 and 8 - Reserved

- Reserved do not modify

Menu Group Extra 2 Menu Options

All of the options in the extra 2 section are currently reserved for future use and expansion.

```
MG001 Extra 2
   [--------]
```

To modify options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Option 1, 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Area Groups

To access the area group programming login using a valid master code and then select [MENU, 2, 3]. The screen displays "Area Group to modify" as shown in the following example.

```
Area group to
modify: AG001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the area groups in the Protege System allow you to configure how a user will interact with the areas in the system and what areas they are able to access.

Selecting an Area Group to Modify

Each area group is assigned a unique area group number from 001 to 250.

```
Area Group to
modify: AG001
```

Type the appropriate 3-digit area group number or use the [🡻] and [🡹] keys to scroll the available area groups. When the desired area group number appears on the screen, press [ENTER] to program the selected area group. The maximum number of area groups that can be programmed is limited by your system's memory and configured profile.

Area Group Name

If the selected area group has a name associated (some area groups do not have a name associated with them) the name programming screen will be shown.

```
AG001 Name
All Areas
```

To scroll area groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected area group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the area group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the area group determines when the area group is valid and if it will use a secondary area group if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
AG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry. (see page 335)

Secondary Area Group

A secondary area group can be selected that will be used when the schedule of the area group that is programmed is not valid. The schedule of the secondary area group must be valid. The secondary group allows very powerful area group controls to be placed on users during certain times of the day.

```
AG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary area group that uses the current area group being edited will perform no function.

Area Group Assignment Blocks 1 to 32

The area group assignment blocks assign an area to the group that is being programmed. Each block is 8 areas and the number of area blocks depends on the number of areas that the system is configured to manage. For example if there are 32 areas there will be 4 blocks of 8 areas. Block 1 option 1 will refer to Area 001 and Block 4 Option 8 will refer to Area 008.

```
AG001 Block 1
   [12345678]
```

To modify the block setting options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Pressing the [ENTER] key will move you to the next block in the area group until you return to the area group selection.

The following table shows the relationship between the block and the area that is being selected for the area group. For example if you want to select Area 23 you would go to block 3 and then change the 7 option.

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
1	Area 001	Area 002	Area 003	Area 004	Area 005	Area 006	Area 007	Area 008
2	Area 009	Area 010	Area 011	Area 012	Area 013	Area 014	Area 015	Area 016
3	Area 017	Area 018	Area 019	Area 020	Area 021	Area 022	Area 023	Area 024
4	Area 025	Area 026	Area 027	Area 028	Area 029	Area 030	Area 031	Area 032
5	Area 033	Area 034	Area 035	Area 036	Area 037	Area 038	Area 039	Area 040
6	Area 041	Area 042	Area 043	Area 044	Area 045	Area 046	Area 047	Area 048
7	Area 049	Area 050	Area 051	Area 052	Area 053	Area 054	Area 055	Area 056
8	Area 057	Area 058	Area 059	Area 060	Area 061	Area 062	Area 063	Area 064

Door Groups

To access the door group programming login using a valid master code and then select [MENU, 2, 4]. The screen displays "Door Group to modify" as shown in the following example.

```
Door Group to
modify: DG001
```

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections. Programming the door groups in the Protege System allow you to configure the doors assigned to a users access level.

Selecting a Door Group to Modify

Each door group is assigned a unique door group number from 001 to 250.

```
Door Group to
modify: DG001
```

Type the appropriate 3-digit door group number or use the [🡻] and [🡹] keys to scroll the available door groups. When the desired door group appears on the screen, press [ENTER] to program the selected door group. The maximum number of door groups that can be programmed is limited by your system's memory and configured profile.

Door Group Name

If the selected door group has a name associated (some door groups do not have a name associated with them) the name programming screen will be shown.

```
DG001 Name
All Doors
```

To scroll door groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected door group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the door group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the door group determines when the door group is valid and if it will use a secondary door group if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
DG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Door Group

A secondary door group can be selected that will be used when the schedule of the door group that is programmed is not valid. The schedule of the secondary door group must be valid or set to none. The secondary door group allows very powerful door group controls to be placed on users during certain times of the day preventing access to certain doors.

```
DG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary door group selection and press [ENTER] to select the door group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary door group that uses the current area group being edited will perform no function.

Door Group Assignment Blocks 1 to 32

The door group assignment blocks assign a door to the group that is being programmed. Each block is 8 doors and the number of door blocks that can be programmed depends on the number of doors that the system is configured to manage. For example if there are 64 doors there will be 8 blocks of 8 doors. Block 1 option 1 will refer to Door 001 and Block 8 Option 8 will refer to Door 064.

```
DG001 Block 1
   [12345678]
```

To modify the block setting options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

Pressing the [ENTER] key will move you to the next block in the door group until you return to the door group selection.

The following table shows the relationship between the block and the door that is being selected for the door group. For example if you want to select Door 12 you would go to block 2 and then press [4] to toggle the option.

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
1	Door 001	Door 002	Door 003	Door 004	Door 005	Door 006	Door 007	Door 008
2	Door 009	Door 010	Door 011	Door 012	Door 013	Door 014	Door 015	Door 016
3	Door 017	Door 018	Door 019	Door 020	Door 021	Door 022	Door 023	Door 024
4	Door 025	Door 026	Door 027	Door 028	Door 029	Door 030	Door 031	Door 032
5	Door 033	Door 034	Door 035	Door 036	Door 037	Door 038	Door 039	Door 040
6	Door 041	Door 042	Door 043	Door 044	Door 045	Door 046	Door 047	Door 048
7	Door 049	Door 050	Door 051	Door 052	Door 053	Door 054	Door 055	Door 056
8	Door 057	Door 058	Door 059	Door 060	Door 061	Door 062	Door 063	Door 064
9	Door 065	Door 066	Door 067	Door 068	Door 069	Door 070	Door 071	Door 072
10	Door 073	Door 074	Door 075	Door 076	Door 077	Door 078	Door 079	Door 080
11	Door 081	Door 082	Door 083	Door 084	Door 085	Door 086	Door 087	Door 088
12	Door 089	Door 090	Door 091	Door 092	Door 093	Door 094	Door 095	Door 096
13	Door 097	Door 098	Door 099	Door 100	Door 101	Door 102	Door 103	Door 104
14	Door 105	Door 106	Door 107	Door 108	Door 109	Door 110	Door 111	Door 112
15	Door 113	Door 114	Door 115	Door 116	Door 117	Door 118	Door 119	Door 120
16	Door 121	Door 122	Door 123	Door 124	Door 125	Door 126	Door 127	Door 128

Door Group Door Schedules

Each door within the door group can be assigned a schedule which will define when the door is valid. A screen will be shown below that will prompt for the door to modify in the door group.

```
DG001 Door to
modify: DR001
```

Type the appropriate 3-digit door number or use the [🡻] and [🡹] keys to scroll the available doors in the door group. When the desired door number appears on the screen, press [ENTER] to program the selected door.

Door Operation Schedule

The door operation schedule is assigned to each door within a door group by selecting the door to edit. By setting a schedule for the door in a door group that door will only be valid if the option is enabled and the schedule is valid. This allows for example a door to be access by a user only between certain times while other doors are always able to be accessed. A schedule is a series of 4 periods of start/end time and days that can be programmed based on a 7 day week and 24 hour clock. A schedule is valid when the time of day falls between any start and end time provided the day of the week is selected and holidays are not affecting the schedule. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
DR001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

A schedule selection of NONE will disable the schedule checking function and allow the door to operate 24HRS within the group provided it has been selected.

Once a schedule has been selected you will be taken back to the door to select screen. For convenience we recommend using the Protege System Management Suite for effective management of door groups and schedules.

Access Level

To access the access level programming login using a valid master code and then select [MENU, 2, 5]. The screen displays "Access Level to modify" as shown in the following example.

```
Access Level to
modify: AL001
```

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections. Programming the access level in the Protege System allows you to configure how user will interact with the system and the options each user will have.

Selecting an Access Level to Modify

Each access level is assigned a unique access level number from 001 to 250.

```
Access Level to
modify: AL001
```

Type the appropriate 3-digit access level number or use the [🡻] and [🡹] keys to scroll the available access levels. When the desired access level number appears on the screen, press [ENTER] to program the selected access level number. The maximum number of access levels that can be programmed is limited by your system's memory and configured profile.

Access Level Name

If the selected access level has a name associated (some access levels do not have a name associated with them) the name programming screen will be shown.

```
AL001 Name
Master
```

To scroll access levels by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected access level use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the access level name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the access level determines when the access level is valid. If the operating schedule is not valid it will use the secondary access level if it is programmed. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
AL001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Access Level

A secondary access level can be selected that will be used when the schedule of the access level that is programmed is not valid. The schedule of the secondary access level must be valid or set to none.

```
AL001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary access level selection and press [ENTER] to select the access level displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary access level with the current access level being edited will perform no function.

Area Arming Group

An access level that has areas assigned to the arm group will only be able to arm those areas unless the user has these areas also assigned to the disarm group.

```
AL001 Arm Grp
All Areas
```

Use the [1] and [3] keys to scroll the area arming group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Area Disarming Group

A user that is assigned an area disarming group will also be able to arm and disarm the areas that belong to this group.

```
AL001 Disarm Grp
None
```

Use the [1] and [3] keys to scroll the area group assigned to the disarm group option and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The area disarming group will allow arming and disarming of all areas within the group. If a user is ONLY allowed to arm an area ensure they are programmed only in the arming group and not the disarming group.

Door Group

A door group can be selected that will be used when the user who is assigned this access level presents their card to a card reader to gain entry to a door. If the door is programmed in to the door group assigned here the user will be granted entry. For more information about door groups refer to the section Door Group Programming (see page 36).

```
AL001 Door Grp
All Doors
```

Use the [1] and [3] keys to scroll the door group selection and press [ENTER] to select the door group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Menu Group

A menu group can be selected that will be used when the user who is assigned this access level logs in to a keypad. A menu group of none will prevent a user from being able to perform any functions on a keypad in the system.

```
AL001 Menu Grp
All Menus
```

Use the [1] and [3] keys to scroll the menu group selection and press [ENTER] to select the menu group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Elevator Car Group

An elevator car group is assigned to an access level to allow a user to access certain elevator cars that are programmed in the system. A user must also have a floor group assigned to gain access to the elevator car.

```
AL001 Elevator
All Cars
```

Use the [1] and [3] keys to scroll the elevator car group selection and press [ENTER] to select the elevator car group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). For information on Elevator Group programming refer to the section Elevator Groups (see page 44).

Elevator Floor Group

An elevator floor group is assigned to an access level to allow a user to access floors within the elevator cars that are assigned.

```
AL001 Floor Grp
All Floors
```

Use the [1] and [3] keys to scroll the elevator floor group selection and press [ENTER] to select the elevator floor group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). For information on Floor Group programming refer to the section Floor Groups (see page 46).

Access Level Miscellaneous Options

These options relate to miscellaneous operation of the access level. These include the operation of PGM activation functions.

```
AL001 Misc
   [--------]
```

To modify options use the relevant key from 1 to 8 to toggle the state of the option.

Option 1 - Activate Access Level PGM on Keypad Access

- Enabled the access level's PGM activates when a user with this access level assigned enters a valid user code on a LCD Keypad.

  For this option to work, the Activate Access Level PGM option must be turned on for the keypad that is being logged into by the user.
- Disabled the access level PGM will perform no function.

Option 2 - Activate Access Level PGM on Card Access

- Enabled the access level's PGM activates when a user with this access level assigned presents a valid card to a card reader.

  For this option to work, the Activate Access Level PGM option must be turned on for the card reader that is being used.
- Disabled the access level PGM will perform no function.

Option 3 - Validate Access Level If Qualify PGM is on

- Enabled the access level will only be valid if the qualify PGM programmed in the qualify PGM entry screen is turned on.

  For this option to work, the Qualify PGM must be programmed with a valid PGM number. If option 3 and 4 are enabled only option 3 will be used.
- Disabled the qualify PGM will not be checked.

Option 4 – Validate Access Level If Qualify PGM is off

- Enabled the access level will only be valid if the qualify PGM programmed in the qualify PGM entry screen is turned off.

  For this option to work, the Qualify PGM must be programmed with a valid PGM number. If option 3 and 4 are enabled only option 3 will be used.
- Disabled the qualify PGM will not be checked.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Activation PGM or PGM Group

You can assign a PGM or PGM group to activate whenever a user performs a valid action from an LCD Keypad or when a user is granted access after presenting their access control card to a reader in the system. The assigned PGM or PGM group only activates if the action performed by the user is permitted by the assigned access level.

```
AL001 Select
pgm: --000:00
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Use the PGM and PGM groups for basic elevator control of up to 8 floors. This provides a very simple elevator control solution. For more complex elevator control use the elevator control features.

Activation PGM Time

You can override the programmed activation time for a PGM by setting an activation time in the access level.

```
AL001 PGM On
time: 00000 secs
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Qualify PGM

You can assign a PGM to be used to qualify the access level. This can be used to prevent the access level from operating denying a user access to the system. Programming a qualify PGM also requires the appropriate option to be set for the way the qualification will be validated.

```
AL001 Qualify
pgm: --000:00
```

To modify the PGM, use the settings as explained in section Entering PGM (see page 336).

User Status

To access the user status menu login using a valid master code and then select [MENU, 2, 6]. The screen displays "Select user to view" as shown in the following example.

```
Select user to
view: UN00001
```

When you press the [ENTER] key the screen will change and display the last area that the selected user is presently in. It will then provide a scrolling display with options that are available. The different screens are described in the following sub-sections.

User Status Display

When the user is selected the screen will change and display the user that you selected last area that they entered.

- The display will show the user name and then the first line of the text explaining the current location of the selected user.

```
Master
Last entered
```

- The display will then scroll to the next display showing the area name that the user is presently in. If the display shows the area "None" the user is considered to be outside of the system.

```
into the area
None
```

- The final screen will display the reset options so that this user can be reset to a known state and gain access. A user can be reset if they have entered or exited an area without presenting their card generating an anti-passback violation.

```
Press [1] to
reset user.
```

Elevator Groups

To access the elevator group programming login using a valid master code and then select [MENU, 2, 7]. The screen displays "Elevator Grp to modify" as shown in the following example. An elevator group is used to allow users access to certain groups of elevators within a building. By programming an elevator group and a floor group you can limit a user to specific floors on specific elevators.

```
Elevator Grp to
modify: EG001
```

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections. Programming the elevator groups in the Protege System allow you to configure the elevator cars that can be assigned to a user's access level.

Selecting an Elevator Group to Modify

Each elevator group is assigned a unique elevator group number from 001 to 250.

```
Elevator Grp to
modify: EG001
```

Type the appropriate 3-digit elevator group number or use the [🡻] and [🡹] keys to scroll the available elevator groups. When the desired elevator group appears on the screen, press [ENTER] to program the selected door group. The maximum number of elevator groups that can be programmed is limited by your system's memory and configured profile.

Elevator Group Name

If the selected elevator group has a name associated (some elevator groups do not have a name associated with them) the name programming screen will be shown.

```
EG001 Name
All Elevators
```

To scroll elevator groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected elevator group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the elevator group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the elevator group determines when the elevator group is valid and if it will use a secondary elevator group if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
EG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Elevator Group

A secondary elevator group can be selected that will be used when the schedule of the elevator group that is programmed is not valid. The schedule of the secondary elevator group must be valid or set to none. The secondary elevator group allows very powerful elevator group controls to be placed on users during certain times of the day preventing access to certain elevators.

```
EG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary elevator group selection and press [ENTER] to select the elevator group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary elevator group that uses the current elevator group being edited will perform no function.

Elevator Group Assignment Blocks 1 to 32

The elevator group assignment blocks assign an elevator car to the group that is being programmed. Each block is 8 elevators and the number of elevator blocks that can be programmed depends on the number of elevators that the system is configured to manage. For example if there are 16 elevators there will be 2 blocks of 8 elevators. Block 1 option 1 will refer to Elevator 001 and Block 2 Option 8 will refer to Elevator 016.

```
EG001 Block 1
   [12345678]
```

To modify the block setting options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the elevator for the block.

Pressing the [ENTER] key will move you to the next block in the elevator group until you return to the elevator group selection.

The following table shows the relationship between the block and the elevator that is being selected for the elevator group. For example if you want to select Elevator 12 you would go to block 2 and then press [4] to toggle the option.

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
1	Elevator 001	Elevator 002	Elevator 003	Elevator 004	Elevator 005	Elevator 006	Elevator 007	Elevator 008
2	Elevator 009	Elevator 010	Elevator 011	Elevator 012	Elevator 013	Elevator 014	Elevator 015	Elevator 016
3	Elevator 017	Elevator 018	Elevator 019	Elevator 020	Elevator 021	Elevator 022	Elevator 023	Elevator 024
4	Elevator 025	Elevator 026	Elevator 027	Elevator 028	Elevator 029	Elevator 030	Elevator 031	Elevator 032

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
5	Elevator 033	Elevator 034	Elevator 035	Elevator 036	Elevator 037	Elevator 038	Elevator 039	Elevator 040
6	Elevator 041	Elevator 042	Elevator 043	Elevator 044	Elevator 045	Elevator 046	Elevator 047	Elevator 048
7	Elevator 049	Elevator 050	Elevator 051	Elevator 052	Elevator 053	Elevator 054	Elevator 055	Elevator 056
8	Elevator 057	Elevator 058	Elevator 059	Elevator 060	Elevator 061	Elevator 062	Elevator 063	Elevator 064
9	Elevator 065	Elevator 066	Elevator 067	Elevator 068	Elevator 069	Elevator 070	Elevator 071	Elevator 072
10	Elevator 073	Elevator 074	Elevator 075	Elevator 076	Elevator 077	Elevator 078	Elevator 079	Elevator 080
11	Elevator 081	Elevator 082	Elevator 083	Elevator 084	Elevator 085	Elevator 086	Elevator 087	Elevator 088
12	Elevator 089	Elevator 090	Elevator 091	Elevator 092	Elevator 093	Elevator 094	Elevator 095	Elevator 096
13	Elevator 097	Elevator 098	Elevator 099	Elevator 100	Elevator 101	Elevator 102	Elevator 103	Elevator 104
14	Elevator 105	Elevator 106	Elevator 107	Elevator 108	Elevator 109	Elevator 110	Elevator 111	Elevator 112
15	Elevator 113	Elevator 114	Elevator 115	Elevator 116	Elevator 117	Elevator 118	Elevator 119	Elevator 120
16	Elevator 121	Elevator 122	Elevator 123	Elevator 124	Elevator 125	Elevator 126	Elevator 127	Elevator 128

Floor Groups

To access the floor group programming login using a valid master code and then select [**MENU, 2, 8**]. The screen displays "Floor Group to modify" as shown in the following example. An elevator group is used to allow users access to certain groups of elevators within a building. By programming a elevator group and floor group you can limit a users access.

```
Floor Group to
modify: FG001
```

Every time you press the [**ENTER**] key, the next screen appears. The different screens are described in the following sub-sections. Programming the elevator groups in the Protege System allow you to configure the floor groups that can be assigned to a users access level.

Selecting a Floor Group to Modify

Each floor group is assigned a unique floor group number from 001 to 250.

```
Floor Group to
modify: FG001
```

Type the appropriate 3-digit floor group number or use the [🡻] and [🡹] keys to scroll the available floor groups. When the desired floor group appears on the screen, press [**ENTER**] to program the selected floor group. The maximum number of floor groups that can be programmed is limited by your system's memory and configured profile.

Floor Group Name

If the selected floor group has a name associated (some floor groups do not have a name associated with them) the name programming screen will be shown.

```
FG001 Name
All Floors
```

To scroll floor groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected floor group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the floor group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the floor group determines when the floor group is valid and if it will use a secondary floor group when the operating schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
FG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Floor Group

A secondary floor group can be selected that will be used when the schedule of the floor group that is programmed is not valid. The schedule of the secondary floor group must be valid or set to none. The secondary floor group allows very powerful floor group controls to be placed on users during certain times of the day preventing access to certain doors.

```
FG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary floor group selection and press [ENTER] to select the floor group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary floor group that uses the current area group being edited will perform no function.

Floor Group Assignment Blocks 1 to 16

The floor group assignment blocks assign a floor to the group that is being programmed. Each block is 8 floor and there 16 floor blocks that can be programmed.

```
FG001 Block 1
   [12345678]
```

To modify the block setting options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

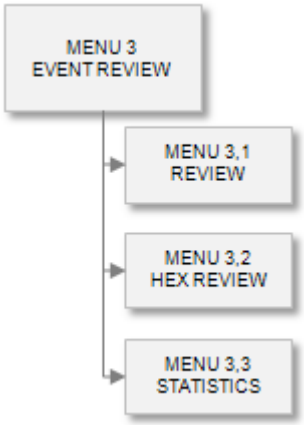
Pressing the [ENTER] key will move you to the next block in the floor group until you return to the floor group selection.

The following table shows the relationship between the block and the floor that is being selected for the floor group. For example if you want to select Floor 12 you would go to block 2 and then press [4] to toggle the floor.

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
1	Floor 001	Floor 002	Floor 003	Floor 004	Floor 005	Floor 006	Floor 007	Floor 008
2	Floor 009	Floor 010	Floor 011	Floor 012	Floor 013	Floor 014	Floor 015	Floor 016
3	Floor 017	Floor 018	Floor 019	Floor 020	Floor 021	Floor 022	Floor 023	Floor 024
4	Floor 025	Floor 026	Floor 027	Floor 028	Floor 029	Floor 030	Floor 031	Floor 032
5	Floor 033	Floor 034	Floor 035	Floor 036	Floor 037	Floor 038	Floor 039	Floor 040
6	Floor 041	Floor 042	Floor 043	Floor 044	Floor 045	Floor 046	Floor 047	Floor 048
7	Floor 049	Floor 050	Floor 051	Floor 052	Floor 053	Floor 054	Floor 055	Floor 056
8	Floor 057	Floor 058	Floor 059	Floor 060	Floor 061	Floor 062	Floor 063	Floor 064
9	Floor 065	Floor 066	Floor 067	Floor 068	Floor 069	Floor 070	Floor 071	Floor 072
10	Floor 073	Floor 074	Floor 075	Floor 076	Floor 077	Floor 078	Floor 079	Floor 080
11	Floor 081	Floor 082	Floor 083	Floor 084	Floor 085	Floor 086	Floor 087	Floor 088
12	Floor 089	Floor 090	Floor 091	Floor 092	Floor 093	Floor 094	Floor 095	Floor 096
13	Floor 097	Floor 098	Floor 099	Floor 100	Floor 101	Floor 102	Floor 103	Floor 104
14	Floor 105	Floor 106	Floor 107	Floor 108	Floor 109	Floor 110	Floor 111	Floor 112
15	Floor 113	Floor 114	Floor 115	Floor 116	Floor 117	Floor 118	Floor 119	Floor 120
16	Floor 121	Floor 122	Floor 123	Floor 124	Floor 125	Floor 126	Floor 127	Floor 128

Events

To access the event review menu, login using a valid code that is allowed event menu access and then select [MENU, 3].



You can then select the event review function that you want to perform on your Protege System. The event menu contains three menu items.

Event Review

To access the event review screen select [MENU, 3, 1]. The screen will show the latest event that has occurred on the system at the time you selected the event review menu item.

```
*Event Menu*
1. Review
```

The event that you are viewing is displayed will consume more than the display is able to show. The event will be split across 4 screens, each screen can be scrolled from left to right using the [🡐] and [🡒] keys.

Event Review Display

When the hex display is selected it will show the data of the event in hexadecimal in the following format. To move between the display screens press [🡐] and [🡒]. To move to the next event in the event review log buffer the [🡓] and [🡑] keys.

- The display will show the time the event occurred and the first portion of the event on the display.

  ```
  Wed 19:56:50 Use
  r Master At KP00
  ```

- Pressing the [🡒] key will move you to the next display screen shows the previous screens bottom line moved to the top and then the rest of the event information on the bottom line.

  ```
  r Master at KP00
  1 Menu 003
  ```

- Pressing the [🡒] key once more will move to the final display for the event.

  ```
  1 Menu 003
  ```

You can scroll back to the other screens by pressing the [🡐] or you can move to the next event by pressing the [🡓] and [🡑] keys.

Hex Review

To access the hex event review screen select [MENU, 3, 2]. The Hex Review screen will show the event information in a machine readable hexadecimal format. This information is primarily used for the verification of third party, OEM and external software that is used to access the Protege System event structure. For more information on event codes, event formats and the meaning of the data structures refer to appendix *Event Code and Formats*.

```
*Event Menu*
2. Hex Review
```

The screen will show the latest event that has occurred on the system at the time the event review menu item was selected. The display will show this event information in a hexadecimal format.

Hex Review Display

When the hex display is selected it will show the data of the event in hexadecimal in the following format. To move between the display screens press [🡐] and [🡒]. To move between the events stored in the event review buffer use the [🡓] and [🡑] keys.

- The display will show the memory location, event code and the time that the event code occurred in the system. In the screen shown below the memory address is 0x441A:A6D4, the event code is 0x030C and the time the event occurred was 19:26:58 and 9ms.

  ```
  441A:A6D4 [030C]
  19:26:58.09
  ```

- Pressing the [🡒] key will move you to the next display screen that shows the data that the event occurred and the day of the week it occurred on.

  ```
  441A:A6D4 [030C]
  10/12/2004-03
  ```

- Pressing the [🡒] key once more will move to the final display that contains the data. The data format is a complex structure and covered in detail in the Event Code Section.

  ```
  441A:A6D4 [030C]
   [00030012001A]
  ```

You can scroll back to the other screens by pressing the [🡐] or you can move to the next event by pressing the [🡓] and [🡑] keys.

Statistics

To access the event statistics screen select [MENU, 3, 3]. The event statistics screen will show the current event stats for the Protege System. This information is primarily used for the verification of third party, OEM and external software that is used to access the Protege System event structure however some information may be informative to the general user.

```
*Event Menu*
3. Statistics
```

Selecting the menu will display the first statistics screen. The screens can be scrolled using the [🡓] and [🡑] keys.

Statistics Display

The event statistics show the current status of the event buffer in the system. To move between the statistics display use the [🡓] and [🡑] keys.

- The display will show the storage buffer memory location.

  ```
  Storage Buffer
  Start 449C19A1
  ```

- Pressing the [↑] key will move you to the next display that will show the storage buffer end memory address.

  ```
  Storage Buffer
  End 49132AC6
  ```

- Pressing the [↑] key once more will move to memory address pointed to by the current head pointer setting.

  ```
  Current Pointer
  Head 4632AC16
  ```

- Pressing the [↑] key once more will move to memory address pointed to by the current tail pointer setting.

  ```
  Current Pointer
  Tail 4632AC16
  ```

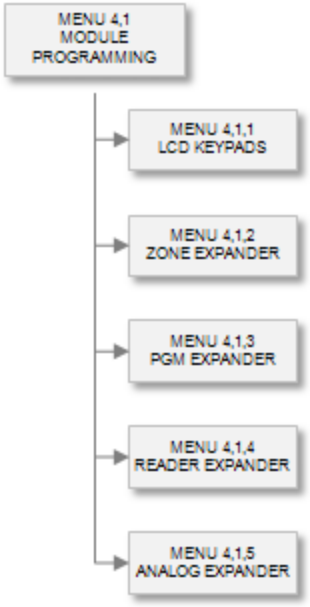
- Pressing the [↑] key once more will move to event count and event buffer wrap settings. The buffer will in most cases ALWAYS be wrapped unless the system has recently been defaulted this is the normal operation of the event buffer and log functions.

  ```
  Current Count
  Count 03962 Wr Y
  ```

You can scroll back to the other statistic screens by pressing the [←] or you can move to the next event by pressing the [↓] and [↑] keys.

Modules

To access the module programming login using a valid installer code and then select [MENU, 4, 1]. You will then have a menu of modules that you can program in the Protege System. Modules are an important part of the system and are used to connect the system to Users (LCD Keypad Expander), Zones (Zone Expander), Card Reading Devices (Reader Expander) and Programmable Outputs (PGM Expander).



LCD Keypad

To access the LCD keypad module programming login using a valid installer code and then select [MENU, 4, 1, 1]. The screen displays "LCD keypad to modify" as shown in the following example.

```
LCD Keypad to
modify: KP001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the LCD Keypad allows you to set the polling time of the module as well as options related to the control of information and the display seen by users on the keypad.

When programming modules some options are processed at the module, for these options to operate correctly a network update must be performed and the keypad must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced Menu Section (see page 201).

Modifying some settings within a keypad may prevent a user from gaining access to the keypad. It is possible that you lock yourself out of the system, ensure that you understand the options that you are setting and that you always have a system keypad or are able to login remotely using the Protege System Management Software.

Selecting a Keypad to Modify

Each keypad is assigned a unique address from 001 to 250. Programming the address of the LCD Keypad Module (PRT-KLCD) is covered in the installation instructions included with your PRT-KLCD LCD Keypad Module.

```
LCD Keypad to
modify: KP001
```

Type the appropriate 3-digit LCD Keypad address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [ENTER] to program the selected LCD Keypad. The maximum number of keypads that can be programmed is limited by your system's memory and configured profile.

Displaying Selected Keypad Information

It is possible to show the current keypad details (registration, online and version information) from the keypad selection display.

```
LCD Keypad to
modify: KP001
```

Type the appropriate 3-digit LCD Keypad address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [ARM] key display information on the selected LCD Keypad. The screen will now display information about the keypad that you have selected. Press any other key to return to the keypad selection window.

```
DE-34-5C-77 [4B]
V 1.15 0622   RO
```

The display above represents the following information for the selected keypad:

DE-34-5C-77	Serial Number of the registered keypad at this address.
[4B]	The current polling timeout value.
V 1.15	Software version of the registered keypad.
0622	Software build number.
R	The keypad is registered (* will indicate no keypad registered)
O	The keypad is online (* will indicate the keypad is offline)

To view the IP address of the module press the [🡹] key from this view. If the module is connected over the RS-485 LAN "---.---.---.---" will be displayed.

To list all offline or online modules refer to the section Module Network Functions (see page 201).

Special functions are provided to update and update reset a module individually by using a shortcut key directly from the keypad selection screen.

Key	Function
[STAY]	Pressing the **[STAY]** key will update the keypad number that is currently displayed in the module selection window. This will program the module WITHOUT resetting the module.
[FORCE]	Pressing the **[FORCE]** key will update and the keypad number that is currently displayed in the module selection window. This will program the module and then restart the module.

Module Polling Time

The polling time defines how often the LCD Keypad checks in with the Protege System Controller. If a LCD Keypad fails to check in, it triggers its associated communications failure trouble zone (KPxxx:08) and the trouble zone for a general module communications failure.

To enter a polling time (008 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the LCD Keypad polling time is set to 250 seconds. Setting a polling time below 60 seconds should only be done for keypads that are in a non-secure area.

```
KP001 Polling
time: 250 secs
```

For UL and ULC listed installations you MUST set the polling time to 180 seconds or less.

Keypad Primary Area

The primary area for the keypad is the area that the keypad will display first on all area display modes. The primary area should belong to the keypad's area group, if any area actions are to be performed on the keypad. For more information on area security refer to the Area Security section (see page 16).

```
KP001 Primary
*Area 001
```

Use the [1] and [3] keys to scroll the primary area selection. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Menu Group

Users can only access a menu assigned to the keypad if the same menu is also assigned to the user. This is also applicable if a menu is assigned to a user, but not to the keypad, the user cannot have access to the menu on the keypad. If you select "None", the user has access to all menus defined by the user's menu group.

```
KP001 Menu Grp
None
```

Use the [1] and [3] keys to scroll the menu group selection. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Area Group

Users can only access an area assigned to the keypad if the same area is also assigned to the user's arm and/or disarm area group. For more information on which areas are displayed by the keypad refer to the Area Security section (see page 16).

```
KP001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area group selection. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Control Door

The keypad control door configured will be is used by the keypad when the door control option is enabled. This allows a door to be unlocked (similar to a request to exit) by pressing and holding the [FUNCTION] key for two seconds.

```
KP001 Ctrl Door
None
```

Use the [1] and [3] keys to scroll the door selection. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Auto Logout Time

When the user does not perform any action on the keypad for the time programmed in the logout time the keypad will automatically log the user out. Programming the option Never Logout should be avoided unless for training or demonstration purposes.

```
KP001 Logout
10 Sec
```

Use the [1] and [3] keys to scroll the auto logout time selection. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Dual User Entry Time

When the keypad is set to require dual-code entry, the dual-code entry time determines how long the users have to enter both codes. Dual code entry is primarily used for the control of ATM and Banking applications. For example, if the time is set to 025 seconds, the dual-code master and dual code provider must successfully enter their codes within 25 seconds in order to gain access. The dual-code can be overridden only by a user that has the dual-code override option set (Super User Option).

```
KP001 Dual
time: 020 secs
```

To enter a dual user entry time (001 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Keypad Invalid Code Lockout Time

If the Lockout option is enabled for the selected keypad and the maximum number of incorrect user codes (PIN Numbers) is reached (3 Times), the time programmed here defines how long the keypad will be locked out. During this period, the keypad will display the lockout message and ignore all key entries or login attempts by ay user. A lockout time of 0 seconds will disable this function regardless of the lockout option setting.

```
KP001 Invalid
time: 060 secs
```

To enter a lockout time (001 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333).

Keypad Smoke Detector Reset PGM

The PGM that is programmed as the keypad smoke detector reset PGM will be activated when a user press's the [CLEAR + ENTER] keys together. The selected PGM should have a time programmed of 5 to 10 seconds, for information on setting a PGM activation time refer to the PGM Programming section (see page 108).

```
KP001 Smoke
pgm: -----:--
```

To enter a smoke detector PGM, use the keypad as explained in section Entering PGM and PGM Groups (see page 336).

Keypad Module Options

Options that relate to the keypad module can be set using option entry.

```
KP001 Module
   [1-34----]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Beep on Key Press

- Enabled the keypad will NOT beep when a key is pressed.
- Disabled the keypad will generate a beep tone each time a key is pressed.

Option 2 - Zone Duplex Operation

- Enabled the keypad will enable the *Duplex Zone* option making it possible to connect four zone inputs to the keypad.
- Disabled the keypad will use the standard zone configuration settings.

Option 3 - Keypad Lockout

- Enabled the keypad will lockout any user activity for the programmed lockout time if three invalid PIN numbers are entered. This option will have no affect if the lockout time is programmed to 0 seconds.
- Disabled the keypad will perform no action on an invalid PIN.

Option 4 - Keypad Lockout

- Enabled the keypad will allow the [CLEAR] / [X] key to disable the beeper on the keypad. You must hold the key for two seconds.
- Disabled the [CLEAR] / [X] will not perform any action.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Keypad Display Options

The following options determine which screens will be displayed when the keypad is offline. The keypad is offline when no valid user code (PIN) has been entered. By default the keypad will display the system message programmed in to the panel configuration settings.

```
KP001 Display
   [1-------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

If all message options are disabled the LCD Keypad will display a standard system is ready message on the display.

Option 1 - System Message Display

- Enabled the keypad will display the text programmed in the panel system message setting.
- Disabled the keypad will not display the system text message.

Option 2 - Primary Area Status Display

- Enabled the keypad will display the status of the primary that is assigned to the keypad.
- Disabled the keypad will not display the primary area status.

Option 3 - Area Group Status Display

- Enabled the keypad will display the status of the area's that are assigned in the area group. Each area is presented on screen and can be scrolled using the [🡻] and [🡹] keys.
- Disabled the keypad will not display the area group status.

Option 4 - Trouble Display

- Enabled the keypad will lockout any user activity for the programmed lockout time if three invalid PIN numbers are entered. This option will have no affect if the lockout time is programmed to 0 seconds.
- Disabled the keypad will perform no action on an invalid PIN.

Option 5 - Bypassed Zone Display

- When enabled the keypad will display the message zone(s) bypassed when a zone has been bypassed in the system or primary area depending on the setting of option 7. Bypassed zones can be viewed by going to the bypass view menu [MENU, 5, 2]. This option can be programmed to only show the primary area bypassed zones by setting option 7.
- Disabled the keypad will not show the bypassed zones message.

Option 6 - Alarm Memory Display

- When enabled the keypad will display the message alarm(s) in memory. Alarms can be viewed by going to the alarm view menu [MENU, 5, 1]. This option can be programmed to only show the primary area alarms by setting option 7.
- Disabled the keypad will show not show the alarm memory status.

Option 7 - Display Only Primary Area

- When enabled with option 6 being enabled the keypad will only display the bypassed zone status and alarm memory for the primary area of the keypad.

  Setting this option with option 7 means that ONLY the primary area's alarms is shown. In which case, the alarm message is cleared ONLY if the primary area's memory is acknowledged.

  If option 7 is not turned on then ANY area that has an alarm stored in memory is shown and ALL the areas' memory must be acknowledged before this message is cleared.
- Disabled the keypad will display the alarm memory and bypassed zones in the system.

Option 8 - Display Area Defer Arming Warnings

- When enabled the keypad will allow defer messages to be shown on the keypad for any area that is in the defer mode and the keypad is part of the defer warning keypad group.
- Disabled the keypad will not display any defer messages regardless of the defer area keypad group.

Keypad Access Options

Options that relate to the keypad access control functions and some specific area control menu settings.

```
KP001 Access
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Unlock Controlled Door

- Enabled the keypad will allow a user to unlock the controlled door by pressing the [FUNCTION] key.
- Disabled the keypad performs no action when the function key is pressed and held. The function key may still be used for home automation or control functions if enabled for the keypad.

Option 2 - Strict Primary Area Status Display

- Enabled the keypad will only display the primary area and will not show ANY other areas regardless of the programmed options for the logged in user or the keypad security settings.
- Disabled the keypad will function normally using the area configuration and user area settings.

Option 3 - 24 Hour Area Access

- Enabled the keypad will allow the 24Hr status screen of an area to be accessed by pressing the [🡐] key when the user is logged in and at the area display screen. The user must have the 24Hr menu option set.
- Disabled the keypad will not display the 24 Hour area status screen.

Option 4 - Area Group Access

- Enabled the keypad will allow the area group access screen to be accessed by pressing the [➔] key when the user is logged in and at the area display screen.
- Disabled the keypad will not allow access to the area groups screen.

Option 5 - Unlock Assigned Door Offline

- Enabled the keypad will allow the [FUNCTION] key to be pressed and held generating an unlock request for the assigned door. This can be programmed to allow a door to be controlled from a local keypad without the addition of a separate REX input.
- Disabled the keypad will allow the door to be unlocked offline.

Option 6 - 8 - Reserved

- Reserved do not modify

Keypad Input Options

Input options which relate to the keypad.

Option 1 - Activate Access Level PGM Only on Valid Access

- Enabled, the users access level PGM will activate after they have logged into the keypad, only if they have a valid menu group and can remain logged in to the keypad.
- Disabled, the users access level PGM will not activate (unless Option 2 is selected).

Option 2 - Always Activate Access Level PGM

- Enabled, the users access level PGM will activate after they have logged into the keypad, even if they do not have a valid menu group or ability to control other features through the keypad.
- Disabled, the users access level PGM will not activate (unless Option 1 is selected).

Options 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Enabling/disabling or modifying the settings of reserved options is not recommended.

Keypad Offline Menu Options

These options turn on or off the menus that are available when the keypad is logged out or offline. The keypad is logged out or offline when no valid user code (PIN) has been entered. It is important to note that even if a menu cannot be accessed online through this keypad (see menu groups); it is possible that it could still be accessed through the offline menu if the following options are turned on. In the same instance a user can be able to access a menu online but not offline.

```
KP001 Offline
   [-2-4----]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Automation Menu

- Enabled the keypad will allow access to the Automation Menu if no user is logged in and a user press's the [MENU] key.
- Disabled the keypad will not allow access to the Automation Menu offline.

Option 2 - View Trouble Menu

- Enabled the keypad will allow access to the View Trouble Menu if no user is logged in and a user press's the [MENU] key.
- Disabled the keypad will not allow access to the View Trouble Menu offline.

Option 3 - Event Review Menu

- Enabled the keypad will allow access to the Event Review Menu if no user is logged in and a user press's the [MENU] key.
- Disabled the keypad will not allow access to the Event Review Menu offline.

Option 4 - Keypad Information Menu

- Enabled the keypad will allow access to the Keypad Information Menu if no user is logged in and a user press's the [MENU] key. It is recommended to leave this option enabled.
- Disabled the keypad will not allow access to the Keypad Information Menu offline.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Zone Expander

To access the Zone Expander module programming login using a valid installer code and then select [MENU, 4, 1, 2]. The screen displays "Zone exp to modify" as shown in the following example.

```
16 Zone Exp to
modify: ZX001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the Zone Expander allows you to set the polling time of the module and power supply options.

When programming modules some options are processed at the module, for these options to operate correctly a network update must be performed and the zone expander must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced menu section (see page 201).

Selecting a Zone Expander to Modify

Each zone expander is assigned a unique address from 001 to 250. Programming the address of the Zone Expander Module (PRT-ZX16) is covered in the installation instructions included with your PRT-ZX16 Zone Expander Module.

```
16 Zone Exp to
modify: ZX001
```

Type the appropriate 3-digit Zone Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [ENTER] to program the selected Zone Expander module. The maximum number of Zone Expanders that can be programmed is limited by your system's memory and configured profile.

Displaying Selected 16 Zone Expander Information

It is possible to show the current 16 Zone Expander registration and information details (registration, online and version) from the 16 zone expander selection display.

```
16 Zone Exp to
modify: ZX001
```

Type the appropriate 3-digit 16 Zone Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press the [ARM] key to display information on the selected 16 Zone Expander. The screen will now display information about the 16 Zone Expander that was selected. Press any other key to return to the 16 Zone Expander selection window.

```
92-A8-90-C2 [9F]
V 1.04 1833   RO
```

The display above represents the following information for the selected keypad:

92-A8-90-C2	Serial Number of the registered keypad at this address.
[9F]	The current polling timeout value.
V 1.04	Software version of the registered keypad.
1833	Software build number.
R	The expander is registered ('*' will indicate no expander registered)
O	('*' will indicate the expander is offline)

To view the IP address of the module press the [↑] key from this view. If the module is connected over the RS-485 LAN "---.---.---.---" will be displayed.

To list all offline or online modules refer to the Module Network Functions (see page 201).

Special functions are provided to update and update reset a module individually by using a shortcut key directly from the keypad selection screen.

Key	Function
[STAY]	Pressing the [STAY] key will update the zone expander number that is currently displayed in the module selection window. This will program the module WITHOUT resetting the module.
[FORCE]	Pressing the [FORCE] key will update and init the zone expander number that is currently displayed in the module selection window. This will program the module and then restart the module.

Zone Expander Polling Time

The polling time defines how often the Zone Expander checks in with the Protege System Controller. If a Zone Expander fails to check in, it triggers its associated communication failure trouble zone (ZXxxx:08) and the trouble zone for a general module communications failure.

To enter a polling time (008 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the Zone Expander polling time is set to 250 seconds. Setting a polling time below 60 seconds should only be done for zone expanders that are in a non-secure area.

```
ZX001 Polling
time: 250 secs
```

For UL and ULC listed installations you MUST set the polling time to 180 seconds or less.

Zone Expander Module Options

Options that relate to the zone expander module can be set using option entry.

```
ZX001 Module
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - High Current Charging

- Enabled the zone expander will enable 700mA charging in the power supply system.
- Disabled the zone expander will enable 350mA charging in the power supply system.

Option 2 - Bell Over Current Requires Acknowledge

- Enabled the bell over current condition will remain until the trouble condition is acknowledged in the system controller at which point all bells (if more than one bell has a problem) will be cleared and reset.

When installing a system to conform to UL or ULC requirements this option must be enabled.

- When the option is disabled and a bell over current condition occurs the bell output will be turned off. It will be turned on one minute later, if the problem still exists it will be turned off again, this process is repeated until the bell is deactivated by the area or other function within the system.

Option 3 – Use Alternate Resistors

- Enabled the zone expander will use alternate EOL configured resistors (2K2 and 6K8).
- Disabled the zone expander will use the normal 1K and 1K resistor configuration.

Option 4 – Invert Module Tamper

- Enabled the zone expander will invert the module tamper input allowing a normally open (door closed) tamper switch to be used.
- Disabled the zone expander will use the standard normally closed (door closed) tamper switch.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

PGM Expander

To access the PGM Expander module programming login using a valid installer code and then select [**MENU, 4, 1, 3**]. The screen displays "PGM exp to modify" as shown in the following example.

```
16 PGM Exp to
modify: PX001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the PGM Expander allows you to set the polling time of the module and power supply options.

When programming modules some options are processed at the module, for these options to operate correctly a network update must be performed and the zone expander must be registered and online.

Updating modules can be accessed by selecting [**MENU, 4, 8, 1, 3**], you can also check the status of your modules by selecting [**MENU, 4, 8, 1, 1**] for all modules presently offline and [**MENU, 4, 8, 1, 2**] for all online modules. For more information refer to the Advanced Menu section (see page 201).

Selecting a PGM Expander to Modify

Each PGM expander is assigned a unique address from 001 to 250. Programming the address of the PGM Expander Module (PRT-PG16) is covered in the installation instructions included with your PRT-PG16 PGM Expander Module.

```
16 PGM Exp to
modify: PX001
```

Type the appropriate 3-digit PGM Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [**ENTER**] to program the selected PGM Expander module. The maximum number of PGM Expanders that can be programmed is limited by your system's memory and configured profile.

Displaying Selected 16 PGM Expander Information

It is possible to show the current 16 PGM Expander registration and information details (registration, online and version) from the 16 PGM expander selection display.

```
16 PGM Exp to
modify: PX001
```

Type the appropriate 3-digit 16 PGM Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press the [ARM] key to display information on the selected 16 PGM Expander. The screen will now display information about the 16 PGM Expander that was selected. Press any other key to return to the 16 Zone Expander selection window.

```
11-14-72-B9 [23]
V 1.05 2404   RO
```

The display above represents the following information for the selected keypad:

11-14-72-B9	Serial Number of the registered keypad at this address.
[23]	The current polling timeout value.
V 1.05	Software version of the registered keypad.
2404	Software build number.
R	The PGM expander is registered ('*' will indicate no expander registered)
O	The PGM expander is online ('*' will indicate the expander is offline)

To view the IP address of the module press the [🡹] key from this view. If the module is connected over the RS-485 LAN "---.---.---.---" will be displayed.

To list all offline or online modules refer to the Module Network Functions (see page 201).

Special functions are provided to update and update reset a module individually by using a shortcut key directly from the keypad selection screen.

Key	Function
[STAY]	Pressing the [STAY] key will update the PGM expander number that is currently displayed in the module selection window. This will program the module WITHOUT resetting the module.
[FORCE]	Pressing the [FORCE] key will update and init the PGM expander number that is currently displayed in the module selection window. This will program the module and then restart the module.

Module Polling Time

The polling time defines how often the PGM expander module checks in with the Protege System Controller. If a PGM expander fails to check in, it triggers its associated communication failure trouble zone (PXxxx:08) and the trouble zone for a general module communications failure.

To enter a polling time (008 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the PGM expander polling time is set to 250 seconds. Setting a polling time below 60 seconds should only be done for PGM expanders that are in a non-secure area.

```
PX001 Polling
time: 250 secs
```

For UL and ULC listed installations you MUST set the polling time to 180 seconds or less.

PGM Expander Module Options

Options that relate to the PGM expander module can be set using option entry.

```
PX001 Module
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - High Current Charging

- Enabled the high current charging option will set 700mA charging in the power supply system.

  For PGM expanders that do not have a power supply this option performs no function.
- Disabled the high current option will set the standard 350mA charging rate in the power supply system.

Option 2 – Invert Module Tamper

- Enabled the PGM expander will invert the module tamper input allowing a normally open (door closed) tamper switch to be used.
- Disabled the PGM expander will use the standard normally closed (door closed) tamper switch.

Option 3 – Stage PGM On/Off

- Enabled the PGM expander will not activate any two local PGMs within 50ms of each other. E.g. If PGM's 1 to 4 were activated at the same time the PX16 would activate PGM 1 first then delay 50ms and activate PGM 2, continuing like this until all 4 PGMs were activated.
- Disabled the PGM expander will turn on or off all PGM's instantly.

Option 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Reader Expander

To access the Reader Expander module programming login using a valid installer code and then select [MENU, 4, 1, 3]. The screen displays "Reader exp to modify" as shown in the following example.

```
2 Reader Exp to
modify: RD001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the Reader Expander allows you to set the polling time of the module, power supply options and the configuration of the readers with associated doors.

When programming modules some options are processed at the module, for these options to operate correctly a network update must be performed and the zone expander must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced Menu section (see page 201).

Selecting a Reader Expander to Modify

Each Reader expander is assigned a unique address from 001 to 250. Programming the address of the Reader Expander Module (PRT-RDI2, PRT-RDM2, PRT-RDS2 and PRT-RDE2) is covered in the installation instructions included with your Reader Expander Module.

```
2 Reader Exp to
modify: RD001
```

Type the appropriate 3-digit Reader Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [ENTER] to program the selected Reader Expander module. The maximum number of Reader Expanders that can be programmed is limited by your system's memory and configured profile.

Displaying Selected 2 Reader Expander Information

It is possible to show the current 2 Reader Expander registration and information details (registration, online and version) from the 2 Reader Expander selection display.

```
2 Reader Exp to
modify: RD001
```

Type the appropriate 3-digit 2 Reader Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press the [ARM] key to display information on the selected 2 Reader Expander. The screen will now display information about the 2 Reader Expander that was selected. Press any other key to return to the 2 Reader Expander selection window.

```
11-14-72-B9 [23]
V 1.31 2404 M RO
```

The display above represents the following information for the selected keypad:

11-14-72-B9	Serial Number of the registered 2 Reader Expander at the selected address.
[23]	The current polling timeout value.
V 1.05	Software version of the registered keypad.
2404	Software version build number.
M	This is the module type that is registered at this location. M - Mini 2 Reader Expander S - Standard 2 Reader Expander I - Intelligent 2 Reader Expander E - Ethernet 2 Reader Expander
R	The 2 Reader expander is registered. ('*' will indicate no expander registered)
O	The 2 Reader expander is online. ('*' will indicate the expander is offline)

To view the IP address of the module press the [🡹] key from this view. If the module is connected over the RS-485 LAN "---.---.---.---" will be displayed.

To list all offline or online modules refer to the Module Network Functions (see page 201).

Special functions are provided to update, update reset a module and request offline events from a module. In the case of a update or update reset this occurs for the individual module however pressing the memory key will start the event request process for the by using a shortcut key directly from the keypad selection screen.

Key	Function
[STAY]	Pressing the [STAY] key will update the zone expander number that is currently displayed in the module selection window. This will program the module WITHOUT resetting the module.
[FORCE]	Pressing the [FORCE] key will update and init the zone expander number that is currently displayed in the module selection window. This will program the module and then restart the module.
[MEMORY]	Pressing the [MEMORY] key will start the system controller in the offline event update mode. This forces the controller to request all offline events from the Intelligent or Ethernet Reader Expanders. Pressing the [MEMORY] key while the system controller is already updating the network or performing other functions the [MEMORY] key will not have any function.

Module Polling Time

The polling time defines how often the Reader Expander module checks in with the Protege System Controller. If a Reader Expander fails to check in, it triggers its associated communication failure (RDxxx:16) trouble zone and the trouble zone for a general module communications failure.

To enter a polling time (008 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the Reader Expander polling time is set to 250 seconds. Setting a polling time below 60 seconds should only be done for Reader Expanders that are in a non-secure area.

```
RD001 Polling
time: 250 secs
```

For UL and ULC listed installations you MUST set the polling time to 180 seconds or less.

Reader Expander Module Options

Options that relate to the reader expander module can be set using option entry.

```
RD001 Module
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 334).

Option 1 - High Current Charging

- Enabled the high current charging option will set 700mA charging in the power supply system of the reader expander.

  For reader expanders that do not have a power supply this option performs no function.
- Disabled the reader expander will set the standard 350mA charging in the power supply system.

Option 2 - Multiple Reader Connected to Port 1

- Enabled the reader will process the multiplexed reader inputs on Port 1 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader.
- Disabled the reader port 1 interface will operate as a single reader input.

Option 3 - Multiple Reader Connected to Port 2

- Enabled the reader will process the multiplexed reader inputs on Port 2 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader.
- Disabled the reader port 2 interface will operate as a single reader input.

Option 4 – Use Alternate Resistors

- Enabled the reader expander will use alternate EOL configured resistors (2K2 and 6K8).
- Disabled the reader expander will use the normal 1K and 1K resistor configuration.

Option 5 – Invert Module Tamper

- Enabled the reader expander will invert the module tamper input allowing a normally open (door closed) tamper switch to be used.
- Disabled the reader expander will use the standard normally closed (door closed) tamper switch.

Option 6, 7 and 8 - Reserved

- Reserved do not modify

Reader Port 1 Mode

The reader mode setting determines what function the reader attached to port one will perform.

```
RD001 R1 Mode
Access
```

Use the [1] and [3] keys to scroll the reader mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Operating Mode	Operation
Access	The reader expander port is used to control access through doors. You must configure the door that is controlled by this reader expander. This mode should also be used if control of a lobby or elevator call button is required. To control a elevator car use the Elevator Mode.
Elevator	The reader expander is used to control access to floors within an elevator. You must configure the elevator number that is connected to the reader.
Area Control	The reader expander input is used to ONLY control an area for arming and disarmed. Please note that this can be achieved using the Access Mode as well by integrating the alarm and access control systems.

Reader Port 1 Controlled Door

The reader controlled door setting sets the door that the reader on port one will provide card and control information to. It is possible that more than one reader has the same controlled door (Entry and Exit reading configuration).

```
RD001 R1 Door
*Door 001
```

Use the [1] and [3] keys to scroll the available door settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 1 Controlled Area

The reader controlled area setting sets the area that the reader on port one will control if the reader mode is set as area control. If area control is selected the reader can not be used for other functions. If you want to disarm and arm areas while using the reader to access the door (integrated access and alarm) refer to the Reader Misc Options section (see page 73).

```
RD001 R1 Area
None
```

Use the [1] and [3] keys to scroll the available area settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 1 Elevator Car

The reader elevator car is used when the reader port 1 mode of operation is configured for Elevator Control mode. When configuring the elevator control mode you must also configure the elevator number for the reader expander that the floor control relays are located on, this is typically the same reader expander that the card reader is connected to. For information on programming the elevator car refer to the Elevator Programming Section (see page 141).

```
RD001 R1 ElvNum
None
```

Use the [1] and [3] keys to scroll the available elevators. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 1 Reading Format

The reading format is used to inform the reader expander what type of card readers are connected to the reader port one. The reader expander supports nearly all publicly available protocols and some special protocols. Any 26 or 37 bit card reader that conforms to the standard format specification will work on the PRT-RDI2 Reader Expander.

```
RD001 Format
26 Bit
```

Use the [1] and [3] keys to scroll the available card reader format settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Format	Description
None	The reader port is disabled and will not perform any function or accept any data from an external device.
26 Bit Wiegand	The industry standard 26 bit format consisting of 8 site code/facility bits and 16 bits of card information. The most common format used in the access control industry.
37 Bit Wiegand	The 37 bit format consists of 4 blocks of 8 bits of data with individual parity bits and 1 overall odd parity at the end of the data. This is commonly used with older HID and Indala style readers.
Keyscan 36 Bit	A proprietary format used by HID Readers that are re-branded for with the Keyscan Corporation of Canada and implemented through out North America.
NCS 25/29 Bit	An older format that allows dual card technology. Northern Control Systems 25 Bit Swipe and 29 Bit Swipe cards.
Northern 34 Bit	Northern Computers proprietary 34 Bit Format.
Kantech 32 Bit	Kantech Systems from Canada. A 32 Bit format sometimes referred to as KSF 32 or Kantech Secure Format.
STID ISO T2	STID of Europe ISO compliant track 2 magnetic card format used for hotels and various other hospitality establishments. Uses the first 8 digits on the card.
Sentrax 9000 T2	A track 2 magnetic card format utilized in New Zealand by the Sentrax T2 Access Control System. Uses an 8 digit site code and 10 digit card number encoded with expiration and utility codes. This format ONLY decodes the Facility and Card numbers.
Propel Systems T2	A track 2 format used through out Asia proprietary based for Propel Systems Sdn Bhd of Kuala Lumpur. Uses a 4 digit site code and 5 digit card number on a track 2 magnetic format card.
40 Bit Wiegand	A 40 Bit Wiegand format used in some older model readers which implements a 12 bit site code and 16 bit card number.
Mirage 33 Bit	A 33 Bit format implemented in the Mirage readers, has a 8 bit site code and 16 bit card number.
Motorola 27 Bit	A 27 Bit format that has 9 site code bits and 16 card number bits.
ABA T2	American Banking Association Track 2 magnetic format that uses the data encoded on a standard 16 digit bank card. The data is hashed and then sent to the controller. This prevents the data from being reversed to establish the card number. This format does NOT require a full 16 digits to create the hash.
Multi 26/34 Bit	A multi bit format to allow the operation of both 26 and 34 Bit Cards on the same port. This can also be achieved by using the secondary reader format.
First 4 Track 2	The first 4 digits of a track 2 card will be used as the card number and a site code of 0 will be generated.

Format	Description
Kantech 39 Bit	A Kantech Systems of Canada format that uses 39 bits of information with a 8 bit facility code and 24 bit card number.
Setec 37 Bit	A Setec Card Reader format that is similar to the 37 Bit format however overall parity is used in place of the individual 4 parity bits.
Motorola ABA T2	Motorola Indala produced card readers that were capable of outputting a multiple format. These generated a format similar to the Track 2 format however the number of digits generated was based on the card programming data.
Hotel T2	An encrypted format used for the hotel industry and prevents the creation of cards. The hotel format can be used with MANY key and lock manufactures. The Hotel Format is not widely used and now slowly being replaced by Smart Card technology. We recommend that this format is not used and is included for legacy implementations.
32 Bit	A straight 32 bit format consisting of a single card serial number and is typically used by Mifare reading devices when outputting data. This can also be sent using the 34 Bit formats.
32 Bit (Rev)	Identical to the 32 Bit format above however the data is sent in reverse order from Bit 32 to Bit 0.
WSE 34 Bit	Westinghouse Security Electronics format. A 34 bit format based on 16 Digit Family number and 16 Digit Card Number.
HID 32 Bit	HID 32 Bit format has no parity and data is generated as a complete 32 Bit data block.
First 6 Track 2	The first 6 digits of a track 2 card will be used as the card number and a site code of 0 will be generated.
30 Bit	The 30 Bit format consists of 2 14 bit blocks with parity and a 8 digit facility code and 20 digit card number. Not a common format and is typically found on older Smart Card readers.
37 Bit	The 37 bit format is different to the first format and of 1 block of 35 bits of data which is broken in to a 20 bit card number and 15 bit site code. This is commonly used with older HID readers.
36 Bit	A standard 36 Bit format which consists of 4 8 bit blocks each with a parity bit. This is commonly used with the Dallas one wire and Kwik Key products.
Rusco 40 Bit	A Casi Rusco 40 Bit format used on the smart card readers produced by Casi Rusco and WSE. The format will output a 24 bit card number and 10 bit site code.
ABA BIN T2	American Banking Association Track 2 magnetic format that uses the BIN (Bank Identification Number) stored in the first 4 digits as the card number. This format can be used to allow entry in to Bank ATM Foyers. By putting an access level on the cards they can also be used to prevent access at certain times and can be used to activate the lighting in the ATM area when presented.
ABA Card T2	American Banking Association Track 2 magnetic format that uses the data encoded on a standard 16 digit bank card. The data is hashed and then sent to the controller. This prevents the data from being reversed to establish the card number. This format is the same as the ABA T2 format however it strictly requires a 16 Digit Card to be presented for the format to operate.
NCS 29 Bit	An older format that is used by Northern Control Systems and is a 29 Bit Format.
HID 26/34 Bit	A dual format consisting of the standard 26 Bit and Standard 34 Bit formats.
HID 34 Bit	A standard HID format consisting of a 16 digit site code and a 16 digit card number with parity calculated on the end two bits.

Format	Description
Auto Wiegand	Automatically selects the best available Wiegand format from the formats to decode the card.
Auto Magnetic	Automatically selects the best available Magnetic Card format from the formats to decode the card data.
36 Bit (IEI)	A standard 36 Bit Output format that is compatible with the IEI keypads, this allows wiegand data to be received from the keypad as a card number. This format can also be used with compatible card reading devices.
34 Bit (Pass)	Decodes the Pass Point 34 Bit Cards used on the HID Card Readers in to the correct large card number 32 bits and standard site code.
34 Bit (Pass NP)	Decodes the Pass Point 34 Bit Cards used on the HID Card Readers however skips the parity validation on the data stream to allow the Nano Prox card readers to be retrofitted to new or existing doors that use the Pass Point cards.
Any Bit (Raw)	Any Bit format decodes ANY wiegand data stream up to 64 bits and then presents this to the system using the multiple decoding display. The display contains encoded data based on the raw data stream sent by the card reader. This allows ANY wiegand reader to operate on the Protege System in a native data format. This format will decode the data explicitly and can be used to verify wiegand data streams.
26 Bit (NP)	Decodes a standard 26 bit wiegand data stream however skips the parity validation portion of the wiegand data. This format can be used when certain card formats have parity detection reversed or if the parity calculation deviates from the standard.
34 Bit (NP)	Decodes a standard 34 bit wiegand data stream however skips the parity validation portion of the wiegand data. This format can be used when certain card formats have parity detection reversed or if the parity calculation deviates from the standard.
First 5 Track 2	The first 5 digits of a track 2 card will be used as the card number and a site code of 0 will be generated for the card swipe.
Apollo 44 Bit	Decodes an encrypted 44 bit wiegand data stream from the AMDI Apollo format card readers. The card number received will match the hot stamp card number. Site codes may vary but will typically be the preceding 3 digits.
CANSEC 37 Bit	
Tecom 27 Bit	

If the required format is not shown or the format that you are using is not known try the configuration with Auto Wiegand or Auto Magnetic. If the data fails to decode contact Integrated Control Technology, we can attempt to create or find a format solution for the reading device you are using.

Reader Port 1 Secondary Reading Format

The secondary reading format is used to program an alternate format for the reader expander and has the same options as the standard reader selection. The secondary format will only be used if the first format can not decode the card information that is received by the reader interface.

```
RD001 R1 Format
None
```

Use the [1] and [3] keys to scroll the available card reader format settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

For a list of supported formats refer to the Reader Expander Format Table (see page 67).

Reader Port 1 Reader Type

The reader type informs the reader expander which location of the door the reader is installed that is connected to the reader expander port one. The reader expander uses this information to pass the correct direction of travel to the door control functions. For an access door this should be set to ENTRY reader.

When using the reader with a door that controls an inside or outside area for arming or disarmed or for global anti-passback the ENTRY and EXIT configuration must be set correctly to ensure the correct action is taken by the reader expander.

```
RD001 R1 Type
ENTRY Reader
```

Use the [1] and [3] keys to scroll the available reader type settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Arming Mode	Operation
ENTRY Reader	The reader is located on the outside of the door and is used to enter in to the area that is being protected by the door. This is the default setting and should be set for all general access doors (single reader)
EXIT Reader	The reader is located on the inside of the door and is used to exit out of the area that is being protected by the door. If the reader expander is configured for multiplex reader mode the multiplexed reader is ALWAYS the EXIT reader.

Reader Port 1 Keypad Operation Mode

The keypad operation mode programmed for the reader on port one determines if the reader port has a pin entry device attached or uses a local LCD keypad.

```
RD001 R1 Key Md
None
```

Use the [1] and [3] keys to scroll the available keypad mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Keypad Mode	Operation
None	There is no keypad device connected to or associated with this reader input device.
LCD Keypad	An LCD keypad is used for PIN entry. PIN entry is only possible with the Card and PIN configuration when using an LCD Keypad. To unlock in the PIN Only or Card or PIN modes the unlock shortcut key can be used. The LCD Keypad Address is configured in the next screen.
26 Bit (Site 0)	A 26 Bit Wiegand Keypad is connected in parallel with the Reader Device and has a site code of 0 set for the unit.
ARK-501	A Motorola Format the ARK-501 outputs 8 bits of data for each key that is pressed consisting of the first 4 bits being inverted from the remaining 4. This format requires the user to press the '#' key on completion of the PIN entry.
4 Bit	4 Bits of data is output for each pressed key.
4 Bit Parity	5 Bits of data is output for each pressed key with the last bit being ODD parity on the first 4 bits.
4 Bit Buffered	The number of bits that are sent relate to the key press's multiplied by 4. The data is buffered and only sent when the user of the keypad press's the Enter key on the keypad.
4 Bit Par + Buf	The number of bits that are sent relate to the key press's multiplied by 5, each key press is 4 bits followed by a last parity bit. The data is buffered and only sent when the user of the keypad press's the Enter key on the keypad.
36 Bit (IEI S0)	A 36 Bit Wiegand Keypad format typical of an IEI keypad which can be set to decode PIN numbers from 0-999999.

When a Wiegand 26 Bit or 36 Bit Keypad is used PIN numbers that are prefixed with a 0 can not be used and a maximum pin number of 65533 can be used for 26 Bit and 999999 for 36 Bit. This is a limitation of the 26 Bit and 36 Bit Format and not the Reader Expander. To utilize the full 8 digit capacity for the PIN number of a user and allow prefixed PIN numbers select a PIN device that supports the ARK-501 or Bit Buffered Outputs.

Reader Port 1 LCD Keypad

If the keypad operation mode is set to use one of the selected LCD keypads you can program the address of the keypad to use for pin entry. When using this mode of operation the LCD keypad will present a login message when a valid card is presented that requires pin entry.

```
RD001 R1 Keypad
None
```

Use the [1] and [3] keys to scroll the available keypad mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 1 Multi Badge Operation

The reader port can perform various operations when a user badges their card multiple times. The list below details the modes this can operate in.

When a multi badge operation has taken place the reader expander will beep the buzzer output four times. In area control, if the area is already armed the reader will only beep twice.

```
RD001 Arming
Arm on 2 Reads
```

Use the [1] and [3] keys to scroll the available arming operation settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Mode	Operation
None	No action will be taken by the system for arming an area associated with the door.
Arm on 2 Reads	Two successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
Arm on Card Read and Zone Input 4	Pressing and holding Zone Input 4 (RDXXX:04) while presenting a card will begin arming. Zone 4 must be in an area that is armed to ensure the zone information is transmitted to the system controller. The area armed will depend on the card reader type setting. **This option cannot be used with the PRT-RDM2, Zone 4 is not available on the module. Use another arming method or use the PRT-RDS2 or PRT-RDI2.**
Arm on 3 Reads	Three successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
Toggle Function PGM	Three successive reads from the same user will result in the function PGM state being toggled. If the PGM is currently on it will be turned off and if it is off it will be turned on.
Activate Function PGM	Three successive reads from the same user will result in the function PGM state being turned on

Reader Port 1 Reader Options

Options that directly relate to the control of reader functions.

```
RD001 R1 Option
   [123-5---]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Reader On Unlock and Door Open

- Enabled the reader expander will send card information to the system controller when a door is unlocked or opened. This option is set by default and should be left set if the door controls areas or time and attendance events are required from the reader port
- Disabled the reader performs no action when a card is presented and the door is unlocked or open.

Option 2 - Send Door Monitoring Events

- Enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control).
- Disabled the reader expander will not send any door events.

Option 3 - LED Follow Lock Status

- Enabled the reader will activate the LED outputs on the reader expander when the lock is opened. This option DOES not prevent the outputs from being used to display the area armed or alarm status.
- Disabled the reader will not perform any function on the LED outputs.

Option 4 - Bond Sense Input Enable

- Enabled the magnetic bond sense functions. The magnetic bond sense is a contact that indicates if the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used however the generation of door events should be processed using both inputs.

  When opening either of the two contacts open (Door Contact or Bond Sense Input) the door monitoring will see this as the door being opened and process it accordingly.
- Disabled the reader will not include the bond sense input in the door status processing.

Option 5 - Request To Exit (REX) Enabled

- Enabled the reader expander will generate request to exit events from the REX input on the reader expander.
- Disabled the keypad will not generate any REX events.

Option 6 - Request To Enter (REN) Enabled

- Enabled the reader expander will generate request to enter events from the REN input on the reader expander.
- Disabled no action will be taken for the Request To Enter function.

Option 7 - Generate Format Error Events

- Enabled the reader expander will send a detailed format error to the system controller if it receives information from the reader that does not comply with the programmed format. Format errors include bit count, byte count, parity, checksum and LRC calculation failures.
- Disabled the reader will silently discard any format error. The format error will still be indicated on the reader input data LED.

Option 8 - Intelligent Reader Tamper

- Enabled the reader expander will assume that the external device has smart messaging that allows a communication path to be formed from the reading device (Card Reader) to the reader expander.

This allows the reader expander to monitor the reading device and generate a reader missing alarm (Trouble Zone) if it fails to communicate with the reader expander, allowing the failure to be reported to a monitoring station. For more information refer to the Nano Prox Programming Manual.

- Disabled the intelligent reader mode is disabled.

Reader Port 1 Miscellaneous Options

Options that relate to the miscellaneous reader functions.

```
RD001 R1 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Disarm Area

- Enabled the reader process will disarm the area designated by the reader type (ENTRY or EXIT) and the door configuration programmed (If it has an area on the inside or outside assigned).

  If this option is enabled and the reader is only used for area control then the area disarmed will be the area assigned in the area control setting.
- Disabled the reader will not perform any disarm functions.

Option 2 - Allow User Access if Area Armed

- When the option is enabled the user will be granted access based on the access control configuration only and the area status will not be checked against the user's ability to disarm the area.
- When the option is disabled and the user who is attempting access to a door that has an area assigned that is armed and the user can not disarm the area the user will be denied entry to the door even though they may have the correct door and schedule settings.

Option 3 - Disarm User Area

- Enabled the reader will disarm the user's area when access is granted to the door they are attempting to access. The users area must still be available in the user area group assigned to the users access level.
- Disabled the reader will not perform any user area functions.

Option 4 - Generate Reader Events

- Enabled the reader events will be logged to the event review log.
- Disabled the reader will not log the events to the event review log.

Option 5 - Swap LED Lock Display

- Enabled the LED display associated with the lock status will follow lock output two. Use this option when a reader expander is used in an ENTRY and EXIT configuration and only one lock output is controlling the door.
- Disabled the lock and LED display is processed normally.

Option 6 - Activate Access Level PGM

- Enabled the reader expander will activate the PGM assigned to the users access level that gained access to the door or reader.

  The user must have the allow access level PGM option enabled.
- Disabled the reader will not perform any action on the access level PGM.

Option 7 - Display Card Data

- Enabled the reader expander will display the actual card data received from the reader when the card number is not known. This can be used to interface with custom third party applications that require their own processing of card information. This option is enabled by default and can be used to add card data to a user when operating the Protege System Management Suite Application.
- Disabled the reader will display the card number not found message.

Option 8 - Arm User Area

- Enabled the reader will arm the user's area when they perform a dual presentation of their card to the associated reader. The users area must still be available in the user area group assigned to the users access level for this to correctly operate.
- Disabled the reader will not perform any user area arming functions.

Reader Port 1 Extra Options

Options that relate to the extra reader functions.

```
RD001 R1 Extra
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Entry Blocked Beam Input

- Enabled the reader expander will process the sense input for beam control. Beam control allows the reader expander to control a automatic gate that must have it's contacts held open in the even the pathway is blocked.
- Disabled the reader will not perform beam processing.

Option 2 - Invert Door Contacts

- When the option is enabled the door contact input is inverted. This does not affect the zone input functionality if it is being used.
- Disabled door contact functions normally.

Option 3 - Invert Bond Sensing Input

- Enabled the reader will invert the bond sensing input.
- Disabled bond sensing will operate normally.

Option 4 - Invert Request to Exit Input

- Enabled the reader will invert the request to exit input.
- Disabled REX input will operate normally.

Option 5 - Invert Request to Enter Input

- Enabled the reader will invert the request to enter input.
- Disabled REN input will operate normally.

Option 6 - Request To Exit Operates Always

- Enabled the reader will always allow a request to exit event EVEN if the door is forced open. This will not restart the forced door or the door alarm operation.
- Disabled REX input will operate only when the door is closed.

Option 7 - Recycle Door Open Too Long Timer On Request To Exit Operation

- Enabled the reader will extend the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the request to exit once the door open too long has been entered will require the door to be closed. This option will not affect the ability for the request to exit action to unlock the door.
- Disabled REX input will not alter the door open time once the door as been opened.

Option 8 - Reserved

- Reserved do not modify

Reader Port 1 Process Options

Options that relate to the extra reader functions.

```
RD001 R1 Process
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options *(see page 336)*.

Option 1 – Convert Force to Door Open

- Enabled the reader expander will process door forced open events as door open events.
- Disabled the reader will process forced door events as normal.

Option 2 – Disable Red LED Processing

- Enabled the reader expander will not control the Red LED (L2) and the PGM can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire.
- Disabled the reader will turn on the Red LED when the door is locked.

Option 3 – Disable Green LED Processing

- Enabled the reader expander will not control the Green LED (L1) and the PGM can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire.
- Disabled the reader will turn on the Green LED when the door is unlocked.

Option 4 – Disable Buzzer Processing

- Enabled the reader expander will not control the Buzzer Output (BZ) and the PGM can be used for another function.
- Disabled the reader will control the buzzer output.

Option 5 - 8 - Reserved

- Reserved do not modify

Reader Port 1 Elevator Options

Options that relate to the elevator functions.

```
RD001 R1 Elv Opt
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Invert Floor Relays

- Enabled the reader expander will invert all the relays on the PX16's connected that are used for elevator control.
- Disabled the reader will not invert the relays.

Option 2 – Control on Comm Fail

- Enabled the PX16 used for elevator control will control the state of the relays when they go offline. Option 3 determines the state the relays will go into.
- Disabled the PX16 used for elevator control will not change the state of the relays when they go offline..

Option 3 – Activate on Comm Fail

- Enabled the PX16 will activate the relays when they go offline.
- Disabled the PX16's will deactivate the relays when they go offline.

Option 4 - 8 - Reserved

- Reserved do not modify

Reader Port 1 Function PGM

You can assign a PGM or PGM group that is used by the multiple badge options.

```
RD001 R1 Func
pgm: --000:00
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Reader Port 2 Mode

The reader mode setting determines what function the reader attached to port two will perform.

```
RD001 R2 Mode
Access
```

Use the [1] and [3] keys to scroll the reader mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Operating Mode	Operation
Access	The reader expander port is used to control access through doors. You must configure the door that is controlled by this reader expander. This mode should also be used if control of a lobby or elevator call button is required. To control a elevator car use the Elevator Mode.
Elevator	The reader expander is used to control access to floors within an elevator. You must configure the elevator number that is connected to the reader.
Area Control	The reader expander input is used to ONLY control an area for arming and disarmed. Please note that this can be achieved using the Access Mode as well by integrating the alarm and access control systems.

Reader Port 2 Controlled Door

The reader controlled door setting sets the door that the reader on port two will provide card and control information to. It is possible that more than one reader has the same controlled door (Entry and Exit reading configuration).

```
RD001 R2 Door
None
```

Use the [1] and [3] keys to scroll the available door settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 2 Controlled Area

The reader controlled area setting sets the area that the reader on port two will control if the reader mode is set as area control. If area control is selected the reader can not be used for other functions. If you want to disarm and arm areas and gain access to doors refer to the Reader Misc Options section (see page 73).

```
RD001 R2 Area
None
```

Use the [1] and [3] keys to scroll the available area settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 2 Elevator Car

The reader elevator car is used when the reader port 2 mode of operation is configured for Elevator Control mode. When configuring the elevator control mode you must also configure the elevator number for the reader expander that the floor control relays are located on, this is typically the same reader expander that the card reader is connected to. For information on programming the elevator car refer to the Elevator Programming Section (see page 141).

```
RD001 R2 ElvNum
None
```

Use the [1] and [3] keys to scroll the available elevators. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 2 Reading Format

The reading format is used to inform the reader expander what type of card readers are connected to the reader port one. The reader expander supports nearly all publicly available protocols and some special protocols. Any 26 or 37 bit card reader that conforms to the standard format specification will work on the PRT-RDI2 Reader Expander.

```
RD001 R2 Format
26 Bit
```

Use the [1] and [3] keys to scroll the available card reader format settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

For a list of supported formats refer to the Reader Expander Format Table (see page 67).

Reader Port 2 Secondary Reading Format

The secondary reading format is used to program an alternate format for the reader expander and has the same options as the standard reader selection. The secondary format will only be used if the first format can not decode the card information that is received by the reader interface.

```
RD001 R2 Format
None
```

Use the [1] and [3] keys to scroll the available card reader format settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

For a list of supported formats refer to the Reader Expander Format Table (see page 67).

Reader Port 2 Reader Type

The reader type informs the reader expander which location of the door the reader is installed that is connected to the reader expander port two. The reader expander uses this information to pass the correct direction of travel to the door control functions. For an access door this should be set to ENTRY reader.

When using the reader with a door that controls an inside or outside area or is used for card or key global anti-passback the ENTRY and EXIT configuration must be set correctly.

```
RD001 R2 Type
ENTRY Reader
```

Use the [1] and [3] keys to scroll the available reader type settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Arming Mode	Operation
ENTRY Reader	The reader is located on the outside of the door and is used to enter in to the area that is being protected by the door. This is the default setting and should be set for all general access doors (single reader)
EXIT Reader	The reader is located on the inside of the door and is used to exit out of the area that is being protected by the door. If the reader expander is configured for multiplex reader mode the multiplexed reader is ALWAYS the EXIT reader.

Reader Port 2 Keypad Operation Mode

The keypad operation mode programmed for the reader on port two determines if the reader port has a pin entry device attached or uses a local LCD keypad.

```
RD001 R2 Key Mod
None
```

Use the [1] and [3] keys to scroll the available keypad mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

When a Wiegand 26 Bit Keypad is used PIN numbers that are prefixed with a 0 can not be used and the maximum pin number is limited to 65533. This is a limitation of the 26 Bit Format and not the Reader Expander. To utilize the full 8 digit capacity for the PIN number of a user and allow prefixed PIN numbers select a PIN device that supports the ARK-501 or 4 Bit Output Formats.

Reader Port 2 LCD Keypad

If the keypad operation mode is set to use one of the selected LCD keypads you can program the address of the keypad to use for pin entry. When using this mode of operation the LCD keypad will present a login message when a valid card is presented that requires pin entry.

```
RD001 R2 Keypad
None
```

Use the [1] and [3] keys to scroll the available keypad mode settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port 2 Multi Badge Operation

The reader port can perform various operations when a user badges their card multiple times. The list below details the modes this can operate in.

When a multi badge operation has taken place the reader expander will beep the buzzer output four times. In area control, if the area is already armed the reader will only beep twice.

```
RD001 R2 Badge
None
```

Use the [1] and [3] keys to scroll the available arming operation settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Mode	Operation
None	No action will be taken by the system for arming an area associated with the door.
Arm on 2 Reads	Two successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
Arm on Card Read and Zone Input 8	Pressing and holding Zone Input 8 (RDXXX:08) while presenting a card will begin arming. Zone 8 must be in an area that is armed to ensure the zone information is transmitted to the system controller. The area armed will depend on the card reader type setting.
Arm on 3 Reads	Three successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
Toggle Function PGM	Three successive reads from the same user will result in the function PGM state being toggled. If the PGM is currently on it will be turned off and if it is off it will be turned on.
Activate Function PGM	Three successive reads from the same user will result in the function PGM state being turned on

Reader Port 2 Reader Options

Options that relate to the control of reader functions.

```
RD001 R2 Option
   [123-5---]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Reader On Unlock and Door Open

- Enabled the reader expander will send card information to the system controller when a door is unlocked or opened. This option is set by default and should be left set if the door controls areas or time and attendance events are required from the reader port
- Disabled the reader performs no action when a card is presented and the door is unlock or open.

Option 2 - Send Door Monitoring Events

- Enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control).
- Disabled the reader expander will not send any door events.

Option 3 - LED Follow Lock Status

- Enabled the reader will activate the LED outputs on the reader expander when the lock is opened. This option DOES not prevent the outputs from being used to display the area armed or alarm status.
- Disabled the reader will not perform any function on the LED outputs.

Option 4 - Bond Sense Input Enable

- Enabled the magnetic bond sense functions. The magnetic bond sense is a contact that indicates if the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used however the generation of door events should be processed using both inputs.

  When opening either of the two contacts open (Door Contact or Bond Sense Input) the door monitoring will see this as the door being opened and process it accordingly.
- Disabled the reader will not include the bond sense input in the door status processing.

Option 5 - Request To Exit (REX) Enabled

- Enabled the reader expander will generate request to exit events from the REX input on the reader expander.
- Disabled the keypad will not generate any REX events.

Option 6 - Request To Enter (REN) Enabled

- Enabled the reader expander will generate request to enter events from the REN input on the reader expander.

Option 7 - Generate Format Error Events

- Enabled the reader expander will send a detailed format error to the system controller if it receives information from the reader that does not comply with the programmed format. Format errors include bit count, byte count, parity, checksum and LRC calculation failures.
- Disabled the reader will silently discard any format error. The format error will still be indicated on the reader input data LED.

Option 8 - Intelligent Reader Tamper

- Enabled the reader expander will assume that the external device has smart messaging that allows a communication path to be formed from the reading device (Card Reader) to the reader expander.

  This allows the reader expander to monitor the reading device and generate a reader missing alarm (Trouble Zone) if it fails to communicate with the reader expander allowing the failure to be reported to a monitoring station.
- Disabled the intelligent reader mode is disabled.

Reader Port 2 Miscellaneous Options

Options that relate to the miscellaneous reader functions.

```
RD001 R2 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Disarm Area

- Enabled the reader process will disarm the area designated by the reader type (ENTRY or EXIT) and the door configuration programmed (If it has an area on the inside or outside assigned).

  If this option is enabled and the reader is only used for area control then the area disarmed will be the area assigned in the area control setting.
- Disabled the reader will not perform any disarm functions.

Option 2 – Allow User Access if Area Armed

- When the option is enabled the user will be granted access based on the access control configuration only and the area status will not be checked against the user's ability to disarm the area.
- When the option is disabled and the user who is attempting access to a door that has an area assigned that is armed and the user can not disarm the area the user will be denied entry to the door even though they may have the correct door and schedule settings.

Option 3 - Disarm User Area

- Enabled the reader will disarm the user's area when access is granted to the door they are attempting to access. The users area must still be available in the user area group assigned to the users access level.
- Disabled the reader will not perform any user area functions.

Option 4 - Generate Reader Events

- Enabled the reader events will be logged to the event review log.
- Disabled the reader will not log the events to the event review log.

Option 5 - Swap LED Lock Display

- Enabled the LED display associated with the lock status will follow lock output one. Use this option when a reader expander is used in an ENTRY and EXIT configuration and only one lock output is controlling the door.
- Disabled the lock and LED display is processed normally.

Option 6 - Activate Access Level PGM

- Enabled the reader expander will activate the PGM assigned to the users access level that gained access to the door or reader.

  The user must have the allow access level PGM option enabled.
- Disabled the reader will not perform any action on the access level PGM.

Option 7 - Display Card Data

- Enabled the reader expander will display the actual card data received from the reader when the card number is not known. This can be used to interface with custom third party applications that require their own processing of card information.
- Disabled the reader will display the card number not found message.

Option 8 - Arm User Area

- Enabled the reader will arm the user's area when they perform a dual presentation of their card to the associated reader. The users area must still be available in the user area group assigned to the users access level for this to correctly operate.
- Disabled the reader will not perform any user area arming functions.

Reader Port 2 Extra Options

Options that relate to the extra reader functions.

```
RD001 R2 Extra
   [--------]
```

To modify options, use the keypad as explained in section *Entering Data Options (see page 336).*

Option 1 - Entry Blocked Beam Input

- Enabled the reader expander will process the sense input for beam control. Beam control allows the reader expander to control a automatic gate that must have it's contacts held open in the even the pathway is blocked.
- Disabled the reader will not perform beam processing.

Option 2 - Invert Door Contacts

- When the option is enabled the door contact input is inverted. This does not affect the zone input functionality if it is being used.
- Disabled door contact functions normally.

Option 3 - Invert Bond Sensing Input

- Enabled the reader will invert the bond sensing input.
- Disabled bond sensing will operate normally.

Option 4 - Invert Request to Exit Input

- Enabled the reader will invert the request to exit input.
- Disabled REX input will operate normally.

Option 5 - Invert Request to Enter Input

- Enabled the reader will invert the request to enter input.
- Disabled REN input will operate normally.

Option 6 - Request To Exit Operates Always

- Enabled the reader will always allow a request to exit event EVEN if the door is forced open. This will not restart the forced door or the door alarm operation.
- Disabled REX input will operate only when the door is closed.

Option 7 - Recycle Door Open Too Long Timer On Request To Exit Operation

- Enabled the reader will extend the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the request to exit once the door open too long has been entered will require the door to be closed. This option will not affect the ability for the request to exit action to unlock the door.
- Disabled REX input will not alter the door open time once the door as been opened.

Option 8 - Reserved

- Reserved do not modify

Reader Port 2 Process Options

Options that relate to the extra reader functions.

```
RD001 R2 Process
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Convert Force to Door Open

- Enabled the reader expander will process door forced open events as door open events.
- Disabled the reader will process forced door events as normal.

Option 2 – Disable Red LED Processing

- Enabled the reader expander will not control the Red LED (L2) and the PGM can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire.
- Disabled the reader will turn on the Red LED when the door is locked.

Option 3 – Disable Green LED Processing

- Enabled the reader expander will not control the Green LED (L1) and the PGM can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire.
- Disabled the reader will turn on the Green LED when the door is unlocked.

Option 4 – Disable Buzzer Processing

- Enabled the reader expander will not control the Buzzer Output (BZ) and the PGM can be used for another function.
- Disabled the reader will control the buzzer output.

Option 5 - 8 - Reserved

- Reserved do not modify

Reader Port 2 Elevator Options

Options that relate to the elevator functions.

```
RD001 R2 Elv Opt
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Invert Floor Relays

- Enabled the reader expander will invert all the relays on the PX16's connected that are used for elevator control.
- Disabled the reader will not invert the relays.

Option 2 – Control on Comm Fail

- Enabled the PX16 used for elevator control will control the state of the relays when they go offline. Option 3 determines the state the relays will go into.
- Disabled the PX16 used for elevator control will not change the state of the relays when they go offline..

Option 3 – Activate on Comm Fail

- Enabled the PX16 will activate the relays when they go offline.
- Disabled the PX16's will deactivate the relays when they go offline.

Option 4 - 8 - Reserved

- Reserved do not modify

Reader Port 2 Function PGM

You can assign a PGM or PGM group that is used by the multiple badge options.

```
RD001 R2 Func
pgm: --000:00
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Reader Communication Failure Card Reading Operation

When the reader expander fails to communicate with the system controller it will default to allowing access through the controlled doors based on the offline communication failure configuration and the type of module that has been registered at the reader location. An intelligent reader expander device will always process users based on the internal offline database and the configuration settings have no affect unless the No Cards option is selected.

```
RD001 Offline
All Cards
```

Option	Function
No Cards	Setting no cards will prevent ANY access from a card reader in the event the module fails and goes offline. This is also applicable to the PRT-RDI2 and PRT-RDE2 modules.
All Cards	This will allow ANY card to enter a reader on the PRT-RDM2 and PRT-RDS2 however on the PRT-RDI2 and PRT-RDE2 only cards that have the correct access credentials according to the internal database at the module will be allowed access.
First Ten	This will allow UN00001 to UN00010 to have unlimited access to the reader inputs on the PRT-RDM2 and PRT-RDS2 however on the PRT-RDI2 and PRT-RDE2 only cards that have the correct access credentials according to the internal database at the module will be allowed access.
Site Code	During the operation of the PRT-RDM2 and PRT-RDS2 the application will store the site codes of cards that have been granted access to the door, the site code will be cached for a period of 7 days or until the card is denied access normally. Setting this option will allow ANY card with the same site code to access the readers on the PRT-RDM2 and PRT-RDI2 modules. The PRT-RDI2 and PRT-RDE2 only cards that have the correct access credentials according to the internal database at the module will be allowed access.

Use the [1] and [3] keys to scroll the available offline communication settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Analog Expander

To access the Analog Expander module programming, login using a valid installer code and then select [MENU, 4, 1, 5]. The screen displays "Analog exp to modify" as shown in the following example.

```
Analog Exp to
modify: AE001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the Analog Expander allows you to set the polling time of the module, channel options and the configuration of the differential settings if they are used.

When programming module some options are processed at the module, for these options to operate correctly a network reload or update must be performed and the analog expander must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], reload and restart the module by pressing the [MENU, 4, 8, 1, 4], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced Menu section (see page 201).

Selecting an Analog Expander to Modify

Each analog expander is assigned a unique address from 001 to 250. Configuring the address of the Analog Expander Module (PRT-ADC4 or PRT-DAC4) is covered in the installation instructions included with your PRT-ADC4 Analog Input Expander or PRT-DAC4 Analog Output Expander Module.

```
Analog Exp to
modify: AE001
```

Type the appropriate 3-digit Analog Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press [ENTER] to program the selected Analog Expander module. The maximum number of Analog Expanders that can be programmed is limited by your system's memory and configured profile.

Displaying Selected Analog Expander Information

It is possible to show the current Analog Expander registration and information details (module type PRT-ADC4 or PRT-DAC4, registration, online and version information) from the Analog Expander selection display.

```
Analog Exp to
modify: AE001
```

Type the appropriate 3-digit Analog Expander address or use the [🡻] and [🡹] keys. When the desired address appears on the screen, press the [ARM] key to display information on the selected Analog Expander. The screen will now display information about the Analog Expander that was selected. Press any other key to return to the Analog Expander selection window.

```
11-14-72-B9 [23]
V 1.05 2404 A RO
```

The display above represents the following information for the selected keypad:

11-14-72-B9	Serial Number of the registered 2 Analog Expander at the selected address.
[23]	The current polling timeout value.
V 1.05	Software version of the registered analog expander.
2404	Software version build number.
A	This means an Analog Input (PRT-ADC4) is at this location a 'D' would indicate an Analog Output (PRT-DAC4) module had been registered.
R	The Analog expander is registered. ('*' will indicate no expander registered)
O	The Analog expander is online. ('*' will indicate the expander is offline)

To view the IP address of the module press the [↑] key from this view. If the module is connected over the RS-485 LAN "---.---.---.---" will be displayed.

To list all offline or online modules refer to the Module Network Functions (see page 201).

Special functions are provided to update and update reset a module individually by using a shortcut key directly from the keypad selection screen.

Key	Function
[STAY]	Pressing the [STAY] key will update the analog expander number that is currently displayed in the module selection window. This will program the module WITHOUT resetting the module.
[FORCE]	Pressing the [FORCE] key will update and init the analog expander number that is currently displayed in the module selection window. This will program the module and then restart the module.

Module Polling Time

The polling time defines how often the Analog Expander module checks in with the Protege System Controller. If a Analog Expander fails to check in, it triggers its associated communication failure (AExxx:08) trouble zone and the trouble zone for a general module communications failure.

To enter a polling time (008 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the Analog Expander polling time is set to 250 seconds. Setting a polling time below 60 seconds should only be done for Analog Expanders that are in a non-secure area or are deemed to be high risk.

The analog expansion modules are in communication constantly with the System Controller and therefore it is recommended not to set the poll time below 250 seconds.

```
AE001 Polling
time: 250 secs
```

For UL and ULC listed installations you MUST set the polling time to 180 seconds or less.

Analog Expander Module Options

Options that relate to the Analog expander module can be set using option entry.

```
AE001 Module
   [--------]
```

To modify the module options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Invert Module Tamper

- Enabled the analog expander will invert the module tamper input allowing a normally open (door closed) tamper switch to be used.
- Disabled the analog expander will use the standard normally closed (door closed) tamper switch.

Option 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Analog Expander Channel 1 Options

The channel one options configures the first channel on the Analog Expander. Please not that the settings may not relate to the particular device connected. Some options relate to the PRT-DAC4 Analog Output Expander and others to PRT-ADC4 Analog Input Expander.

The channel options require a module init or module init with reboot to take affect with the exception of the Log Channel Data Option 7, which is a controller based configuration setting.

```
AE001 Ch 1 Opts
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Enable Channel Operation

- Enabled the analog expansion device will process messages according to the options configuration and module type.
- Disabled the channel will perform no function.

Option 2 – Channel Input Output Configuration

- When the option is enabled the input or output will operate in Current Mode and use the 0-20mA and 4-20mA interface.
- Disabled the channel will operate in 0-10V input or output mode.

Option 3 – Preset PRT-DAC4 Output on Power Up

- Enabled and the analog expansion module is a DAC module the output will be preset when it powers up to the setting in option 4.
- Disabled the DAC output will be set to the last known value that it received.

Option 4 – Set to Full Scale Output

- Enabled and option 3 enabled the DAC output will be set to the maximum or full scale deflection.
- Disabled and option 3 enabled the DAC will output a analog value of 0 on the voltage or current outputs.

Option 5 – Reserved

- Reserved do not modify

Option 6 – Differentiate On Send Operation

- Enabled the Analog Input channel will constantly monitor the analog input value for any variance greater than the configured differentiate value set for the channel and then send an update to the system controller.
- Disabled the Input Channel will be sent based on the period configured in the channel time setting.

Option 7 – Log Raw Analog Data

- Enabled the Analog Expander channels when updated either as an input or an output will trigger a log in the event screen with the exact raw value. This is ideal for fault finding HOWEVER should not be left on in a live system as it will fill the event review rapidly.

To log data from a channel for charting and display purposes utilize the log option for variables in the Protege System Management Suite.

- Disabled the data is not logged to the review screen.

Option 8 - Reserved

- Reserved do not modify

Analog Channel 1 Update Time

When the analog input expander is used the channel will generate analog information that is stored in the variable associated with the analog expander. The data can be programmed to be sent in various incremental values. As many elements that are monitored by sensors operate slowly we recommend using the longest times possible. This also reduces the risk of disturbances due to interference as the input is averaged over the period of time being sampled.

```
AE001 Ch 1 Time
30 Secs
```

Use the [1] and [3] keys to scroll the channel time settings. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Analog Channel 1 Differentiate On Send Value

The value that is configured is constantly monitored against the last value that is sent to the system controller and if a change has occurred greater than the amount programmed and differentiate on send option is enabled the channel will send an update and start the comparison process again.

The value that is programmed is an offset of the raw input value to the analog expansion module device. The last sent value is retained and any input is sampled and averaged before being compared to the differentiate value.

```
AE001 Ch 1 diff
value: 000
```

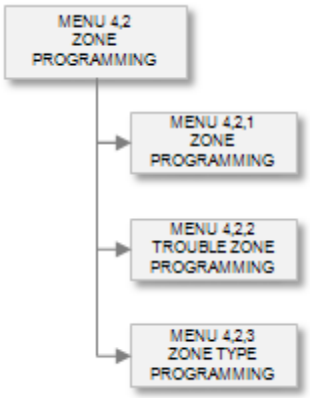
To enter a value (0-255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Programming Analog Channel 2, 3 and 4

The programming screens for channels 2, 3 and 4 are identical to channel one and you will be prompted with each channel screen as you press the [ENTER] key. Each channel operates independently of each other.

Zone Inputs

To access the zone programming, login using the valid installer code and then select [MENU, 4, 2, 1] for zone programming, [MENU, 4, 2, 2] for trouble zone programming and [MENU, 4, 2, 3] for zone type programming. The Zones menu enables you to set up and program all the zones in your system.



Zones and trouble zones can only be programmed when the areas they are assigned to and the area's 24hr processing are disarmed/disabled, refer to Arm and Disarm Operations. If the area or the associated 24hr processing is armed/enabled, you can only view the screens, but not modify the information they contain. A warning will be shown on entering the zone programming indicating that the zone is only able to be viewed and the records are locked.

When selecting a Zone or Trouble Zone the zone address is entered using the Module Type, Module Address and the number of the zone or trouble zone, this is called Protege Object Notation. Information on the Protege Object Notation and how it applies to programmable objects within the Protege System refer to the Object Notation section (see page 330).

For the alarm memory to display a trouble zone when a tamper/short occurs, the 24hr processing must be enabled for at least one of the area's that the zone has been assigned in.

Zone

To access the Zone programming menu login using a valid installer code and then select [MENU, 4, 2, 1]. The screen displays "Select zone to modify" as shown in the following example.

```
Select zone to
modify: CP001:01
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming zones allows you to configure which zones belong in to areas and the options used when the zone is activated.

When programming zones some options are processed at the module, for these options to operate correctly a network update must be performed and the device that the zone is located on must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced Menu Section (see page 201).

Selecting a Zone to Modify

Each zone is assigned a unique identification that uses the Protege Notation.

```
Select zone to
modify: CP001:01
```

Type the appropriate module type, module address and zone number or use the [🡻] and [🡹] keys to scroll the available zones. When the desired zone number appears on the screen, press [ENTER] to program the selected zone number.

Zone Name

If the selected zone has a name associated (some zones do not have a name associated with them) the name programming screen will be shown.

```
CP001:01 Name
*Zone CP001:01
```

To scroll zones by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected zone use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the zone name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Zone Miscellaneous Options

Miscellaneous options for the zone include the configuration of event logging, bypass and arming configurations for the zone.

```
CP001:01 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Zone Event

- Enabled the zone will generate an event whenever it is opened, closed, tampered or shorted.

  The zone will still perform all functions that are programmed if this is not enabled. When using zones as automation zones it is recommended to disable the event logging option to reduce the impact on the event log buffer.
- Disabled the zone will not log an event.

Option 2 - Trouble Condition Display

- When enabled the zone will be monitored for a trouble condition and cause a trouble alarm to be generated. The trouble will be generated only if the zone is either shorted or tampered.
- Disabled the zone is not monitored for trouble conditions.

Option 3 - Bypassing Not Allowed

- Enabled the zone is a high security zone and cannot be bypassed.

  However, the zone can still be force armed if the Force Arming option is turned on. In order to avoid this, and to insure that the zone is not ignored when force arming, the Zone Force Arming option should be turned off in the zone type that is assigned to the zone.
- Disabled the zone can be bypassed.

Option 4 - Bypassing Latched Not Allowed

- Enabled the zone is a high security zone and cannot be latch bypassed (Permanent Bypass).

However, the zone can still be force armed if the Force Arming option is turned on. In order to avoid this, and to insure that the zone is not ignored when force arming, the Zone Force Arming option should be turned off.

- Disabled the zone can be latch bypassed.

Option 5 - Zone State Inverted

- Enabled the zone the will operated in an inverted mode. By default all zones are normally closed, setting this option will change the zone to normally open.

  At least one zone open and close is needed to correctly update the zone state.
- Disabled the zone will operate normally.

Option 6 - Log zone event when bypassed

- Enabled.
- Disabled.

Option 7 - Tamper zone if module offline

- Enabled.
- Disabled.

Option 8 - Zone Lock out

- Enabled, if this Zone triggers an alarm in an area more than the specified number of times then it will be prevented from retriggering further alarms until the area is disarmed then rearmed. This setting does not affect the 24 hour tamper detection of the zone. The number of times the zone can trigger an alarm before lockout occurs can be set under the Zone Lockout Count setting.
- Disabled, the Zone will never be locked out.

Zone Special Options

Special options for the zone include the configuration of special bypass and wiring settings for the zone. When using special EOL resistors the hardware revision of the Controller (PRT-CTRL) and Zone Expander (PRT-ZX16) must be revisions 070 and 040 respectively for the EOL to function. Multiple EOL values for options 5, 6, 7 and 8 are reserved for any module that does not support the multiple EOL options.

```
CP001:01 Special
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Tamper Bypass Allowed

- Enabled the zone will bypass the tamper monitoring of the zone at the time the zone is bypassed.
- Disabled the zone will only bypass the alarm states and a tamper alarm or short will generate a tamper alarm.

Option 2 - No Bypass When Area Armed

- When enabled the zone will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.
- Disabled the zone can be bypassed while it is in an armed condition. This option is not recommended unless it is required for a specific reason.

Option 3 - Zone Uses EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration. If no other EOL option is selected the Zone will operate with 1K+1K resistor values (Default) otherwise the resistor value selected by options 4-7 will override the setting. Only one EOL can be selected and selecting more than one will result in the lowest numbered EOL option being used.
- Disabled the zone will use no EOL resistors.

Option 4 - Zone Uses 6K8 and 2K2 EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration with a 6K8 and 2K2 resistor. For this option to operate you MUST also have option 3 enabled.
- Disabled the zone will use the default EOL resistors if enabled.

Option 5 - Zone Uses 10K and 10K EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration with a 10K and 10K resistor. For this option to operate you MUST also have option 3 enabled.
- Disabled the zone will use the default EOL resistors if enabled.

Option 6 - Zone Uses 2K2 and 2K2 EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration with a 2K2 and 2K2 resistor. For this option to operate you MUST also have option 3 enabled.
- Disabled the zone will use the default EOL resistors if enabled.

Option 7 - Zone Uses 4K7 and 2K2 EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration with a 4K7 and 2K2 resistor. For this option to operate you MUST also have option 3 enabled.
- Disabled the zone will use the default EOL resistors if enabled.

Option 8 - Zone Uses 4K7 and 4K7 EOL Resistors

- Enabled the zone will use the 2 EOL resistor wiring configuration with a 4K7 and 4K7 resistor. For this option to operate you MUST also have option 3 enabled.
- Disabled the zone will use the default EOL resistors if enabled.

When you make a change to the zone options you MUST do a module update for the module the zone is located on. This INCLUDES the controller. You can do this from the Keypad or from the Protege System Management Suite.

Zone Reporting Id

The Zone Reporting Id allows the installer to program any reporting number to any zone. This provides an extremely high level of flexibility to assign true reporting numbers to the zones. A zone that is assigned the same reporting ID as another zone will result in both the zones reporting that ID.

If a zone is assigned an ID number that is higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for that format.

```
CP001:01 Report
id: 00000
```

To enter a value (0-65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a reporting ID of 00000 will result in the default reporting id being used for the service.

Zone First Area Assignment

The zone must be assigned to an area for it to perform any function in the system and a zone can be assigned in up to 4 different areas. A zone can perform a different function in each area. For example a zone can be a delay zone in one area and an instant zone in another.

```
CP001:01 Area 1
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type First Area Assignment

When a zone is assigned to an area the zone must be programmed with the type of zone (Delay, 24HR etc). The Protege System has twelve predefined zone types as well as user definable zone types.

```
CP001:01 Type 1
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Second Area Assignment

The zone must be assigned to an area for it to perform any function in the system and a zone can be assigned in up to 4 different areas. A zone can perform a different function in each area. For example a zone can be a delay zone in one area and an instant zone in another.

```
CP001:01 Area 2
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type Second Area Assignment

When a zone is assigned to an area the zone must be programmed with the type of zone (Delay, 24HR etc). The Protege System has twelve predefined zone types as well as user definable zone types.

```
CP001:01 Type 2
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Third Area Assignment

The zone must be assigned to an area for it to perform any function in the system and a zone can be assigned in up to 4 different areas. A zone can perform a different function in each area. For example a zone can be a delay zone in one area and an instant zone in another.

```
CP001:01 Area 3
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type Third Area Assignment

When a zone is assigned to an area the zone must be programmed with the type of zone (Delay, 24HR etc). The Protege System has twelve predefined zone types as well as user definable zone types.

```
CP001:01 Type 3
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Fourth Area Assignment

The zone must be assigned to an area for it to perform any function in the system and a zone can be assigned in up to 4 different areas. A zone can perform a different function in each area. For example a zone can be a delay zone in one area and an instant zone in another.

```
CP001:01 Area 4
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type Fourth Area Assignment

When a zone is assigned to an area the zone must be programmed with the type of zone (Delay, 24HR etc). The Protege System has twelve predefined zone types as well as user definable zone types.

```
CP001:01 Type 4
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Control PGM or PGM Group

You can assign a PGM or PGM group to activate whenever a zone type process's the zone with the activate zone PGM options enabled. The zone type must have the appropriate zone control PGM options set in the PGM options. A PGM can be assigned to the zone type and to the zone allowing many to one and one to many configurations.

```
CP001:01 Control
pgm: --000:00
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

To activate the Control PGM in a zone the zone type used to process the zone must have the zone control options set. The zone control options are different from the Zone Type control options.

Automation Control Point

An automation control point allows this zone to control an automation point in response to a zone type configuration. The automation point can be programmed to activate when when the zone opens or closes. An automation point can be assigned many different functions such as gardening irrigation, lighting circuits, CBus Circuits and any PGM Output. You must configure the appropriate options to trigger the Automation point in the Zone Type. An automation point can also be triggered from a zone type allowing many too one and one to many configurations.

```
ZT001 Automate
None
```

Use the [1] and [3] keys to scroll the available automation points and press [ENTER] to select the automation point displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Alarm Zone Speed

This determines how long a zone must be open for before an alarm event will be generated. This can be set from 0 seconds up to 1 hour. If the Alarm Zone Speed is set at 0 seconds, the Restore Zone Speed can not be set below 100ms.

```
CP001:01 Alarm
500 msec
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Restore Zone Speed

This determines how long a zone must be closed for before an restore event will be generated. This can be set from 0 seconds up to 1 hour. If the Alarm Zone Speed is set at 0 seconds, the Restore Zone Speed can not be set below 100ms.

```
CP001:01 Seal
500 msec
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Lockout Count

If this Zone triggers an alarm in an area more than the specified number of times then it will be prevented from retriggering further alarms until the area is disarmed then rearmed. The lock out count specifies how many times a Zone can trigger an alarm before being locked out. This count is qualified the Zone Lockout enable flag under the Zone Miscellaneous Options.

```
CP001:01 Lockout
count: 005
```

To modify the Lockout Count (001 to 254), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Trouble Zone

To access the Trouble Zone programming menu login using a valid installer code and then select [MENU, 4, 2, 2]. The screen displays "Trouble zone to modify" as shown in the following example.

```
Trouble zone to
modify: CP001:01
```

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections. Programming trouble zones allows you to configure which trouble zones belong in to areas and the options used when the trouble zone is activated.

When programming trouble zones some options are processed at the module, for these options to operate correctly a network update must be performed and the device that the trouble zone is located on must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Advanced Menu Section (see page 201).

Selecting a Trouble Zone to Modify

Each trouble zone is assigned a unique identification that uses the Protege Notation.

```
Trouble zone to
modify: CP001:01
```

Type the appropriate module type, module address and trouble zone number or use the [🡻] and [🡹] keys to scroll the available trouble zones. When the desired trouble zone number appears on the screen, press [ENTER] to program the selected trouble zone number.

Trouble Zone Miscellaneous Options

Miscellaneous options for the zone include the configuration of event logging, bypass and arming configurations for the zone.

```
CP001:01 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Trouble Zone Event

- Enabled the trouble zone will generate an event whenever it is opened or closed.

  The trouble zone will still perform all functions that are programmed if this is not enabled.
- Disabled the trouble zone will not log an event.

Option 2 - Bypassing Not Allowed

- Enabled the trouble zone is a high security trouble zone and cannot be bypassed.
- Disabled the trouble zone can be bypassed.

Option 3 - Bypassing Latched Not Allowed

- Enabled the trouble zone is a high security trouble zone and cannot be latch bypassed (Permanent Bypass).
- Disabled the trouble zone can be latch bypassed.

Option 4 - Trouble Zone State Inverted

- Enabled the trouble zone will operate in an inverted mode.
- Disabled the trouble zone will operate normally.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Trouble Zone Special Options

Special options for the zone include the configuration of special bypass and wiring settings for the zone.

```
CP001:01 Special
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - No Bypass When Area Armed

- When enabled the zone will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.
- Disabled the zone can be bypassed while it is in an armed condition. This option is not recommended unless it is required for a specific reason.

Option 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Trouble Zone Trouble Group

The high level of flexibility that is provided with the Protege System allows the definition of the trouble type and group that is generated by a trouble zone. Troubles are grouped by a trouble group and then a trouble type within the group. When the trouble zone generates an alarm it will also generate the appropriate trouble condition that is configured. The trouble group and type are used to generate trouble conditions on the keypad and to prevent an area from Arming based on the trouble condition. To view the trouble conditions that are on the panel select the View Menu and select the Trouble View option (see page 267).

```
CP001:01 Group
System Trouble
```

Use the [1] and [3] keys to scroll the available trouble groups that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Group	Description
General Trouble	The General Trouble group consists of the trouble types that are part of the main system operation. Trouble conditions such as AC Failure, Real Time Clock and Bell Output Troubles belong to this group and are assigned the General Trouble Group and the appropriate trouble type from the group by default.
System Trouble	The System Trouble group is used for module related system messages, hardware faults and other system conditions that do not belong in the general trouble group.
Access Trouble	The Access Control trouble group consists of the trouble conditions that are related to access control and door operation these include door forced open, door left open and number of attempts are some of the trouble types.

Trouble Zone Trouble Type

When a trouble zone is assigned to a trouble group it can then have a trouble type within the group assigned.

```
CP001:01 Type
Module Tamper
```

Use the [1] and [3] keys to scroll the available trouble types that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The trouble zone types belong to the trouble groups, selecting a trouble group will allow the appropriate trouble type from that group to be selected. The following trouble types are shown for each of the three groups below.

General Trouble Group

Type	Description
AC Failure	AC Failure has occurred on one or more devices in the system.
Battery Problem	A Low Battery or Missing Battery on one or more devices in the system.
RTC/Clock Loss	The Real Time Clock has not been set since the System Controller has powered up. To reset the associated trouble set the time from the time menu.
Reporting Failure	The System Controller has failed to get a report through to the monitoring station in the programmed number of attempts. This will restore when the next reporting event is successful.
Phone Line Fault	The phone line is either cut or damaged on the system controller.
Zone Fault	A zone in the system is tampered or short circuited.
Fire Loop	A fire zone has a loop fault.
Power Fault	A power problem (Auxiliary, Fuse or Analog) has occurred on the System Controller or a device in the system.
Bell/PGM Fault	The Bell/PGM Output on the system controller or a device in the system has either been disconnected or it has shut down due to excessive current consumption.

System Trouble Group

Type	Description
Module Tamper	A module in the system has been tampered.
Module Loss	A module has failed to communicate with the system controller.
Module Security	A module has attempted to register with the system controller however the system controller is secured.
Hardware Fault	The system controller can not communicate with an accessory interface board or a device that is connected to the system controller has a hardware failure.

Access Trouble Group

Type	Description
Forced Door	A door in the system has been forced open or opened without being accessed correctly.
Door Left Open	A door has been left open past the left open time.
Number Attempts	The number of attempts to gain entry in to a door or keypad devices has been exceeded. The next valid access will reset this trouble condition.
User Denied	A user has been denied entry to a keypad or door.
Unknown Card	An unknown card has been received by the system on a card reader input.
Reader Tamper	A reader input that has been configured for intelligent tamper has generated a tamper condition.

Trouble Zone Reporting Id

The Trouble Zone Reporting Id allows the installer to program any reporting number to any trouble zone. This provides an extremely high level of flexibility to assign true reporting numbers to the trouble zones that are used in a system. A trouble zone that is assigned the same reporting ID as another trouble zone will result in both the trouble zones reporting that ID.

If a trouble zone is assigned an ID number that is higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for that format.

```
CP001:01 Report
id: 00000
```

To enter a value (0-65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a reporting ID of 00000 will result in the default reporting id being used for the service. Using a reporting id above 999 will restrict the ability to use the reporting ID in Contact ID.

Trouble Zone First Area Assignment

The trouble zone must be assigned to an area for it to perform any function in the system. By default ALL trouble zones are assigned to the predefined trouble area which is the last programmable area in the system. A trouble zone can be assigned in up to 4 different areas. A trouble zone can perform a different function in each area.

```
CP001:01 Area 1
Trouble Area
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Type First Area Assignment

When a trouble zone is assigned to an area the zone must be programmed with the type of trouble zone (Trouble Silent, Trouble Bell etc).

```
CP001:01 Type 1
Trouble Silent
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Second Area Assignment

The trouble zone must be assigned to an area for it to perform any function in the system. By default ALL trouble zones are assigned to the predefined trouble area which is the last programmable area in the system. A trouble zone can be assigned in up to 4 different areas. A trouble zone can perform a different function in each area.

```
CP001:01 Area 2
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Type Second Area Assignment

When a trouble zone is assigned to an area the zone must be programmed with the type of trouble zone (Trouble Silent, Trouble Bell etc).

```
CP001:01 Type 2
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Third Area Assignment

The trouble zone must be assigned to an area for it to perform any function in the system. By default ALL trouble zones are assigned to the predefined trouble area which is the last programmable area in the system. A trouble zone can be assigned in up to 4 different areas. A trouble zone can perform a different function in each area.

```
CP001:01 Area 3
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Type Third Area Assignment

When a trouble zone is assigned to an area the zone must be programmed with the type of trouble zone (Trouble Silent, Trouble Bell etc).

```
CP001:01 Type 3
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Fourth Area Assignment

The trouble zone must be assigned to an area for it to perform any function in the system. By default ALL trouble zones are assigned to the predefined trouble area which is the last programmable area in the system. A trouble zone can be assigned in up to 4 different areas. A trouble zone can perform a different function in each area.

```
CP001:01 Area 4
None
```

Use the [1] and [3] keys to scroll the available areas that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Trouble Zone Type Fourth Area Assignment

When a trouble zone is assigned to an area the zone must be programmed with the type of trouble zone (Trouble Silent, Trouble Bell etc).

```
CP001:01 Type 4
None
```

Use the [1] and [3] keys to scroll the available zone types that can be assigned to the trouble zone. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type

To access the Zone Type programming menu login using a valid installer code and then select [MENU, 4, 2, 2]. The screen displays "Zone type to modify" as shown in the following example.

```
Zone Type to
modify: ZT001
```

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections.

Zone Type Name

If the selected zone type has a name associated (some zone types do not have a name associated with them) the name programming screen will be shown.

```
ZT001 Name
Delay
```

To scroll zone types by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected zone type use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the zone name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the zone type determines when the zone type is valid. If the operating schedule is not valid it will use the secondary zone type if it is programmed. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
ZT001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Zone Type

A secondary zone type can be selected that will be used when the schedule of the zone type that is programmed is not valid. The schedule of the secondary zone type must be valid or set to none.

```
ZT001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary zone type selection and press [ENTER] to select the zone type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary zone type with the current zone type being edited will perform no function.

Zone Type Keypad Group

A zone type keypad determines which keypads will be presented with alarm information when the zone that the zone type is assigned generates an alarm.

```
ZT001 Key Grp
None
```

Use the [1] and [3] keys to scroll the available keypad groups and press [ENTER] to select the keypad group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Control Area

A zone type can be programmed to control the arming and disarming state of an area from a zone input (key switch control). The area to be controlled by the zone type must be programmed with the force arming option. Arming using a zone type is deemed to be a unattended arming condition and therefore the system will attempt to arm the area in the force mode.

```
ZT001 Ctrl Area
None
```

Use the [1] and [3] keys to scroll the available area's and press [ENTER] to select the area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Automation Control Point

An automation control point allows this zone type to control an automation point in response to a zone opening or closing. An automation point can be assigned to many different functions such as gardening irrigation, lighting circuits, CBus Circuits and any PGM Output. You must configure the appropriate options to trigger the Automation point.

```
ZT001 Automate
None
```

Use the [1] and [3] keys to scroll the available automation points and press [ENTER] to select the automation point displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Zone Type Alarm Options

Alarm options for the zone type configure the operation of the zone type when an alarm, restore and tamper are generated.

```
ZT001 Alarm
   [12345---]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Process Alarms

- Enabled the zone type will process alarms from the zone that it is assigned.
- Disabled the zone type will perform no function on an alarm being generated.

Option 2 - Process Tamper 24HR Alarm

- Enabled the zone type will process tamper alarms from the zone that it is assigned.
- Disabled the zone type will perform no tamper processing.

Option 3 - Entry Delay

- Enabled the zone type will start an entry delay timer for the assigned area when the zone generates an alarm.
- Disabled the zone type will not perform any entry delay actions.

Option 4 - Entry Delay Follow

- Enabled the zone type will allow this zone to generate alarms during the entry delay however it will generate an alarm if the alarm condition occurs outside the entry delay period.
- Disabled the zone type operates normally.

Option 5 - Exit Delay Follow

- Enabled the zone type will allow this zone to generate alarms during the exit delay however it will generate an alarm if the alarm condition occurs outside the exit delay period.

  Use this feature to prevent 'Sitters' from re-entering a building that is assumed to be secure during a long arming process.
- Disabled the zone type operates normally.

Option 6 - Shorten Exit Delay Timer On Restore

- Enabled the zone type will shorten the exit delay timer on an area to five seconds when the zone restores.

  Use this feature to reduce the arming time of an area.
- Disabled the zone type operates normally.

Option 7 - 24HR Alarm

- Enabled the zone type will generate a 24HR alarm if the zone generates an alarm. The area state will not affect the generation of this alarm.
- Disabled the zone type operates normally.

Option 8 - Fire Alarm

- Enabled the zone type will generate a fire alarm when it is activated. This zone type will also operate similar to the 24HR Alarm option.

  Most smoke detectors use a normally open contact so any zone that is assigned this option must have the inverted state option selected and the EOL resistors option enabled.
- Disabled the zone type operates normally.

Zone Type Report Options

Reporting options for the zone type configure the operation of the zone type when reporting to a communication service and includes options for various other zone type options.

```
ZT001 Report
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Alarm

- Enabled the zone type will generate a reportable alarm message.
- Disabled the zone type does not generate a reportable alarm message.

Option 2 - Report Tamper

- Enabled the zone type will generate a reportable tamper message.
- Disabled the zone type does not generate a reportable tamper message.

Option 3 - Report Bypass

- Enabled the zone type will generate a reportable bypass message.
- Disabled the zone type does not generate a reportable bypass message.

Option 4 - Report Restore

- Enabled the zone type will generate a reportable restore message.
- Disabled the zone type does not generate a reportable restore message.

Option 5 - Stay Zone

- Enabled the zone type will generate an alarm if the area is armed in stay mode. The zone will stay armed. For zones that will be active when an area is armed in stay mode it is recommended to disable the event log for the zone.
- Disabled the zone type operates normally.

Option 6 - Force Zone

- Enabled the zone type will allow the zones it is assigned to be force armed.
- Disabled the zone type operates normally.

Option 7 - No Exit Test

- Enabled the zone type will not verify the status of a zone prior to the area starting to arm. Use this feature to assign zones in exit locations to prevent the area from generating a zone open warning when being armed.
- Disabled the zone type operates normally.

Option 8 - Recycle Zone On Exit Delay

- Enabled the zone type will recheck the zones it is assigned when the area completes the exit delay cycle and if a zone is open recycle the zone to force it in to generating an alarm.

  Use this feature for a zone type used on a zone that may be breached during the exit delay such as a window or door contact.

- Disabled the zone type operates normally.

Zone Type Miscellaneous Options

Miscellaneous options for the zone type configure options for various functions.

```
ZT001 Misc
   [1-3-----]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Generate Siren Bell Output

- Enabled the zone type will activate the siren bell output programmed for the area.
- Disabled the zone type will not generate a bell output.

Option 2 - Restart Siren Bell Timer

- Enabled the zone type will restart the bell timer on each subsequent alarm.
- Disabled the zone type will not alter the bell timer if it is already active.

Option 3 - Save Alarm to Memory

- Enabled the zone type will save an alarm message to the area's alarm memory storage area.
- Disabled the zone type does not save an alarm message.

Option 4 - Disarm Control Area on Restore

- Enabled the zone type will disarm the control area when a zone assigned the zone type restores from an alarm condition.

  Use this feature and the arming control area feature as a on and off key switch arming input.
- Disabled the zone type takes no action on the control area.

Option 5 - Arm Control Area on Alarm

- Enabled the zone type will start arming the control area when a zone assigned the zone type generates an alarm condition.
- Disabled the zone type takes no action on the control area.

Option 6 - Toggle Control Area State On Alarm

- Enabled the zone type will toggle the state of the control area when the zone that is assigned this zone type generates an alarm.
- Disabled the zone type operates normally.

Option 7 - Force Arm Tamper

- Enabled the zone type will allow the zone to be force armed if the zone assigned the zone type is tampered.
- Disabled the zone type operates normally.

Option 8 - Activate Entry PGM For Bell Siren Time Duration

- Enabled the zone type will activate the entry PGM programmed for the area for the duration of the bell siren time.

  Use this feature for a zone that you want to only generate a beeper alarm and assign the entry PGM a keypad beeper pgm. This option will not function if the bell option is enabled.
- Disabled the zone type operates normally.

Zone Type PGM Options

PGM options for the zone type configure options for various functions that control the PGM's programmed in a zone type.

```
ZT001 Pgm Ctrl
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Activate Bypass PGM

- Enabled the zone type will activate bypass PGM for the area if a zone is bypassed.
- Disabled the zone type will not activate the bypass PGM.

Option 2 - Activate Tamper PGM

- Enabled the zone type will activate the tamper PGM for the area if a tamper alarm occurs.
- Disabled the zone type will not activate the tamper PGM.

Option 3 - Activate Memory PGM

- Enabled the zone type will activate the memory PGM for the area if an alarm occurs.

  This option can be used to indicate that an alarm has occurred in the system. Use this feature to display an indication to the users of the system to prevent possible "Sitter and Hostage" situations.

- Disabled the zone type will not activate the memory PGM when an alarm occurs.

Option 4 - Activate Control PGM On Alarm

- Enabled the zone type will activate the control PGM when the zone assigned generates an alarm.
- Disabled the zone type takes no action on the control PGM.

Option 5 - Activate Control PGM On Restore

- Enabled the zone type will activate the control PGM when the zone assigned restores from an alarm.
- Disabled the zone type takes no action on the control PGM.

Option 6 - Deactivate Control PGM On Alarm

- Enabled the zone type will de-activate the control PGM when the zone assigned generates an alarm.
- Disabled the zone type takes no action on the control PGM.

Option 7 - Deactivate Control PGM On Restore

- Enabled the zone type will de-activate the control PGM when the zone assigned restores from an alarm.
- Disabled the zone type takes no action on the control PGM.

Option 8 - Reserved

- Reserved do not modify

Zone Type Automation Options

Automation options for the zone type configure options for various functions that relate to the control of automation control settings. The options to control the 24Hr bell are also located in the Automation options.

```
ZT001 Auto Ctrl
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Activate Automation on Alarm

- Enabled the zone type will activate the automation point when the zone assigned this zone type goes in to alarm.
- Disabled the zone type takes no action on the automation point.

Option 2 - Activate Automation on Restore

- Enabled the zone type will activate the automation point when the zone assigned this zone type goes in to alarm.
- Disabled the zone type takes no action on the automation point.

Option 3 - Deactivate Automation on Alarm

- Enabled the zone type will deactivate the automation point when the zone assigned this zone type goes in to alarm.
- Disabled the zone type takes no action on the automation point.

Option 4 - Deactivate Automation on Restore

- Enabled the zone type will deactivate the automation point when the zone assigned the zone type restores.
- Disabled the zone type takes no action on the automation point.

Option 5 - Toggle Automation State on Alarm

- Enabled the zone type will toggle the current state of the automation number that has been assigned.
- Disabled the zone type takes no action on the automation point.

Option 6 - 24HR Audible If Area Armed

- Enabled the zone type will activate the bell PGM if a 24HR alarm is generated when the area is armed. Please note that this option will be overridden by option 6 and will have no affect.
- Disabled the 24HR will be silent. This will have no affect if option 6 is enabled.

Option 7 - 24HR Always Audible

- Enabled the zone type will always activate the bell PGM for the area if a 24HR tamper alarm occurs. This option will override option 5 when enabled.
- Disabled the 24HR will be silent.

Option 8 - Reserved

- Reserved do not modify

Zone Extra Options

Additional options for setting up the Zone Type.

```
ZT001 Extra
 [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Always Log Zone Event

- Enabled, if the 'Log to Event Buffer' option in the Zone options is deselected, then over-ride this and log the Event anyway.
- Disabled, log the event only as required by other settings

Option 2 - Retrigger PGM time

- Enabled, each time the Zone activates it will restart the associated PGMs time out counter.
- Disabled, the Zone will not retrigger the PGM time.

Options 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Enabling/disabling or modifying the settings of reserved options is not recommended.

Zone Control PGM Options

Zone PGM options for the zone type, configure how the zone type will process the activation of the PGM assigned to the zone (not the zone type).

```
ZT001 Zone Ctrl
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Use Zone Type PGM Time

- Enabled the zone will activate the PGM timed (if a time is programmed) and use the PGM Time Set in the Zone Type. If the zone type does not have a time programmed no time will be used.
- Disabled the zone will activate using the PGM timer if it is set to a value greater than 0.

Option 2 - Activate Control PGM On Alarm

- Enabled the zone type will activate the zone control PGM when the zone assigned generates an alarm.
- Disabled the zone type takes no action on the control PGM.

Option 3 - Activate Control PGM On Restore

- Enabled the zone type will activate the zone control PGM when the zone assigned restores from an alarm.
- Disabled the zone type takes no action on the zone control PGM.

Option 4 - Deactivate Control PGM On Alarm

- Enabled the zone type will de-activate the zone control PGM when the zone assigned generates an alarm.
- Disabled the zone type takes no action on the zone control PGM.

Option 5 - Deactivate Control PGM On Restore

- Enabled the zone type will de-activate when the zone control PGM assigned restores from an alarm.
- Disabled the zone type takes no action on the zone control PGM.

Option 6 – Toggle Zone Control PGM On Restore

- Enabled the zone control PGM will be toggled when the zone goes in to alarm. You can use this option to activate a PGM on alarm and deactivate on the next alarm. This is ideal for lighting control and automation applications.
- Disabled the zone type takes no action on the zone control PGM.

Option 7 and 8 - Reserved

- Reserved do not modify

Reporting Code

Each zone type has a default reporting code already assigned which determines the code that is sent to the central station when an alarm is generated refer to the *Contact ID Codes table*. However, it is possible to change the reporting code of the zones to which this zone type is assigned. This is used when using special reporting formats for example ModBUS Remote uses this to identify special zone points to the remote Protege System Controller.

```
ZT001 Report
code: 255
```

To enter a reporting code (000 to 254), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. By default the Zone Type Reporting Code is set to 255. Setting a value of 255 uses the default reporting code for the zone assigned.

Control PGM or PGM Group

You can assign a PGM or PGM group to activate whenever a zone type process's an alarm or restore for a zone. The zone type must have the control PGM options set in the PGM options.

```
ZT001 Control
pgm: --000:00
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Control PGM Activation Time

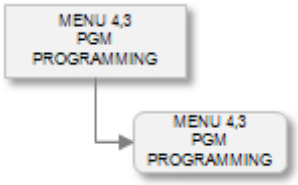
You can override the programmed activation time for a PGM by setting an activation time in the zone type.

```
ZT001 PGM on
time: 00000 secs
```

To modify the PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

PGM Outputs

PGM's are programmable outputs that can change state (ON or OFF) when a specific event occurs in the system. For example, a PGM can be programmed to activate an LED or beeper. To access the PGM programming menu, login using a valid installer code that is allowed PGM programming access and then select [MENU, 4, 3]. The PGM's Menu enables you to set up and program all the PGM's in your system. This includes setting an activation time and special options for each PGM within the Protege System.



When selecting a PGM the PGM address is entered using the Module Type, Module Address and the number of the PGM (Object), this is called Protege Object Notation. Information on the Protege Object Notation and how it applies to programmable objects within the Protege System refer to the Object Notation Section (see page 330).

Every time you press the [ENTER] key, the next screen appears. The different screens are described in the following sub-sections. When programming PGM's some options are processed at the module, for these options to operate correctly a network update must be performed and the device that the PGM is located on must be registered and online.

Updating modules can be accessed by selecting [MENU, 4, 8, 1, 3], you can also check the status of your modules by selecting [MENU, 4, 8, 1, 1] for all modules presently offline and [MENU, 4, 8, 1, 2] for all online modules. For more information refer to the Network Menu Section (see page 201).

To control a PGM for testing purposes refer to the Advanced Programming Section (see page 207).

To control more than one PGM from an event or function refer to the PGM Group Programming Section (see page 108).

Selecting a PGM to Modify

Each PGM is assigned a unique identification that uses the Protege Notation.

```
Select PGM to
modify: CP001:01
```

Type the appropriate module type, module address and PGM number or use the [🡻] and [🡹] keys to scroll the available PGM's. When the desired PGM number appears on the screen, press [ENTER] to program the selected PGM number.

PGM Name

If the selected PGM has a name associated (some PGM's do not have a name associated with them) the name programming screen will be shown.

```
CP001:01 Name
*PGM CP001:01
```

To scroll PGM's by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected PGM use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the PGM name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Activation Schedule

The activation schedule is programmed to activate the PGM at a certain time of the day or to activate the PGM between certain hours. The schedule will be checked at the start and end times and if the start is valid the PGM will be activated, if the end time of the schedule is valid the PGM will be deactivated.

If a PGM is controlled by an operator, user or other function during this activation time and is deactivated it will remain in the deactivated state. Setting the recheck schedule option for the PGM will force the PGM to have the schedule verified every 60 second period. This will prevent the PGM from being controlled manually as the schedule will override the manual operation.

```
CP001:01 Sched
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

PGM Activation Time

Setting an activation time for a PGM will mean that any device controlling the PGM will only activate the PGM for the programmed time.

```
CP001:01 Pgm
time: 00000 secs
```

To enter a activation time (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

PGM Miscellaneous Options

Miscellaneous options for the PGM include the configuration of event logging, schedule and power up configurations for the PGM.

```
CP001:01 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log PGM Event

- Enabled the PGM will generate an event whenever it is activate or deactivated.

  The PGM will still perform all functions that are programmed if this is not enabled. When using PGM's as automation control outputs it is recommended to disable the event logging option to reduce the impact on the event log buffer.
- Disabled the PGM will not log an event.

Option 2 - Verify Schedule State

- When enabled the PGM will re verify the schedule that is programmed every 60 seconds. If the PGM is meant to be activated but is in a deactivated state the system will activate the PGM.
- Disabled the PGM will only activate at the start time and the end time of the programmed schedule.

Option 3 - Change PGM State at Panel Reset

- Enabled the PGM will be set to the state that is selected by option four when the panel is reset or powers up for the first time. By default this option is enabled and all PGM's will be set to the deactivated state.
- Disabled the PGM state will not be changed from when the panel was reset or powered down.

Option 4 - PGM State Setting

- Enabled the PGM will be activated if option three is enabled.
- Disabled the PGM will be deactivated if option three is enabled.

Option 5 - Inverted Operation

- Enabled the PGM will operate inverted. Deactivation will result in the PGM being activated and activation will result in the PGM being deactivated.
- Disabled the PGM will operate normally.

Option 6 - Activate On Module Power Up and Reset

- When enabled the PGM will activate when the module powers up, this will be overridden by the current state that is held in the controller.

  Note that these options are different from the activation and deactivation settings in the miscellaneous section as they relate to the local module PGM's.

- Disabled the PGM will be deactivated by the module at power up.

Option 7 - Control PGM Communications Failure

- Enabled the PGM will be controlled and set to the state that is programmed in the communications state setting Option 4.
- Disabled the PGM state will not be modified during a module communication failure.

Option 8 - Communication State Setting

- Enabled the PGM will be activated if option seven is enabled.
- Disabled the PGM will be deactivated if option seven is enabled.

PGM Extra Options

Extra options are currently reserved.

```
CP001:01 Extra
   [--------]
```

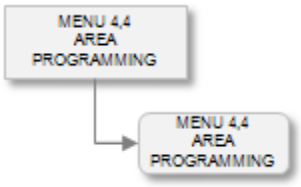
To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1, 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Area

An installation may contain any number of areas or partitions depending on the configuration and size of the system needed. Areas can contain zones and trouble zones that protect the area. Zones can be assigned to as many as four areas and perform a different function in each area individually of the other area's status.



Any area may also contain no zones and be used to control lighting, car parking, user loiter functions, automatic teller machines, banking and money trail control. The area processing is a powerful solution and one of key features of the Protege System.

To access the area programming menu, login using a valid installer code that is allowed area menu access and then select [MENU, 4, 4]. The Areas menu enables you to set up and program all the areas in your system. This includes setting entry and exit delays and special options for each area.

Areas can only be programmed when they are disarmed and the 24hr (Tamper) processing has been disabled, for information on controlling the area refer to the Area Control Section (see page 16). If the area is armed or the 24hr processing is enabled, you can only view the screens, but not modify them.

Selecting an Area to Modify

Each area is assigned a unique area number from 001 to 250. Your system will be limited to specific number of areas that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Select area to
modify: AR001
```

Type the appropriate 3-digit area number or use the [🡻] and [🡹] keys to scroll the available area numbers. When the desired area number appears on the screen, press [ENTER] to program the selected area number. The maximum number of areas that can be programmed is limited by your system's memory and configured profile.

Area Name

If the selected area has a name associated (some areas do not have a name associated with them) the name programming screen will be shown.

```
AR001 Name
*Area 001
```

To scroll areas by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected area use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the area name will be prefixed by an '*' this indicates that the name is an editable name in the system. Some areas do not have names, this is limited by the system memory and the profile configured.

Area Entry Delay Time

Setting an entry delay time for the area allows users that have entered a secured point to have time to disarm the area before the area generates an alarm. Only zones that have a zone type assigned with an entry delay option set will start the entry delay timer for the area.

```
AR001 Entry
time: 060 secs
```

To enter a entry delay time (000 to 250), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Area Exit Delay Time

Setting an exit delay time for the area allows users to exit the area once the arming of the area has begun without triggering an alarm. Zones that are part of the exit route should be programmed with the exit option in the assigned zone type.

```
AR001 Exit
time: 030 secs
```

To enter a exit delay time (000 to 250), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. An exit delay time of 000 seconds will result in the area arming instantly.

Area Siren Bell Time

The bell time determines how long the bell/siren output for the area will remain activated before timing out. If the option to retrigger the bell time is set in the zone type assigned to a zone that is triggered in the area the siren bell time is reloaded on each subsequent alarm activation.

Use the siren bell time and the retrigger bell option from the zone type for smart automation of lighting and building control.

```
AR001 Bell
time: 004 mins
```

To enter a bell siren time (000 to 250 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. A bell siren time of 000 will result in no siren or bell activation.

Intelligent False Alarm Prevention Time

Setting an intelligent false alarm prevention time allows the area to process alarms using smart alarm verification. For an alarm to occur in the area it will require that the same zone generate more than one alarm in a time programmed or that any other zone that is not assigned the intelligent false alarm prevention time generates an alarm.

```
AR001 Intel zone
time: 000 secs
```

To enter an intelligent false alarm prevention time (000 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting the intelligent false alarm prevention time to a value of 000 will result in any intelligent false alarm prevention zone from activating normally.

Re-Arm Delay

Setting the re-arm delay will result in the area automatically re-arming after the re-arm timer has elapsed. This should be programmed for area's used to monitor and control system functions that should not be disarmed.

This is also used to control vault and automatic teller machines when using the banking area functions to prevent an area from being disarmed for longer than a the time programmed.

```
AR001 Re-arm on
time: 030 mins
```

To enter a re-arm delay time (000 to 250 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. For the re-arm timer to operate the re-arm option must be enabled.

Arming/Disarming Schedule

The arming and disarming schedule is programmed so that an area will be armed and disarmed according to a schedule that is assigned.

The area will be disarmed at the start time and armed at the end time of the schedule.

In the case that an area only requires to be disarmed program the start time with the time that is required to disarm and the end time of the schedule with --:--. This will mean the area will automatically disarm at the start time for the programmed days in the period.

Do the same if the area requires to be armed only on schedule by programming the end period with the required time to arm and set the start time to --:--.

```
AR001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Recent Close Time

The recent closing time defines how long the system considers an armed area recently closed. If, after arming the area, an alarm is generated within the programmed period, the Protege System Controller transmits a recent closed message. For this feature to operate correctly the zone must have its report options enabled in the assigned zone type.

```
AR001 Recent cls
time: 000 secs
```

To enter a recent closing delay time (000 to 250 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a value of 000 will result in no recent closing reports being sent for the area.

Disarm Delay Time

The disarm delay time is used in conjunction with the Automatic Teller Machine control and banking control functions. Setting a disarm delay time will cause the area to delay by the programmed delay time any access to the area.

```
AR001 Disarm dly
time: 000 mins
```

To enter a disarm delay time (000 to 250 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Code Delay Time

The code delay time is used in conjunction with the Automatic Teller Machine control and banking control functions. Setting a code delay time will cause the area to wait for a code for the delay by the programmed time.

```
AR001 Code dly
time: 000 secs
```

To enter a code delay time (000 to 250 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Maximum Bypass Count

The bypass count number sets the maximum number of zones that can be bypassed within the programmed area.

```
AR001 Bypass
count: 000
```

To enter a bypass count (000 to 250), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Maximum User Count

The user count defines the maximum number of users that can be in the area at any one time. For example, if the user count is set to 10, then the 11th user who attempts to enter the area is denied access. Typically, the user count feature is used when an area is controlled by an entry and an exit reader. When an access control card is presented to exit the area, the user count goes down. The count is reset to 0 when the area is armed. You can also program the area to auto-arm when the count reaches 0 by enabling the Last User Arm option.

```
AR001 Max user
count: 00000
```

To enter a user count (00000 to 65535 users), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a maximum user count of 0 will result in an unlimited number of users being allowed entry into the area.

Child Area Assignment

The child area is an area dependent on another area (the parent area). For example, if an area is armed, then its child area can also be automatically armed. If you select "None", the area will not have a child area assigned. You can use this option to program a common area as there is no limit to the number of areas containing the same child area. A common area is an area that is the child area of more than one parent area. The common area can only be armed once all of its parent areas are armed.

```
AR001 Child Area
None
```

Use the [1] and [3] keys to scroll the child areas selection and press [ENTER] to select the area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Selecting a child area that is the same area as the area being edited will perform no function in the system.

Area Interlock Group Assignment

An area interlock group can be assigned to an area to prevent it from being armed or disarmed depending on the status of all area's within the assigned interlock group.

```
AR001 Interlock
None
```

Use the [1] and [3] keys to scroll the area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Loiter Time Setting

The loiter time defines how long a user can remain in a specific loiter enabled area. If the loiter time has elapsed and the user is still in the area, the user will be denied access when an attempt is made to exit the area. If the user has not exited the loiter area before the loiter time has elapsed, then the user status must be reset manually from the operator software or local keypad. For this option to operate, the Loiter Mode options must be turned on for the user and a loiter area must be programmed. Furthermore, the area requires an entry and exit reader set with the anti-passback feature to control the user traffic.

```
AR001 Loiter
time: 00000 mins
```

To enter a loiter time (00000 to 65535 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Loiter Area Violation Assignment

The loiter area violation setting is used when a user has violated the loiter configuration for the installation and must be set to an area that they can not exit or enter from for the loiter area. The setting here is typically an area that is not used in the system and is defined as being an invalid area.

```
AR001 Loiter Ar
None
```

Use the [1] and [3] keys to scroll the loiter violation areas selection and press [ENTER] to select the area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Leaving the loiter violation area set to none will allow the user to present their card at a reader that is external to the area (Such as a parking entrance) and be able to regain another period of loiter time for the area programmed if the reader is part of the loiter area.

Bell PGM or PGM Group

You can assign a bell/siren PGM or PGM group to activate whenever the area goes in to alarm. The zone that triggers the alarm must have the bell PGM option enabled for the zone type. The bell/siren PGM and PGM Group will be deactivated when the bell timer times out or when the area is disarmed, the bell/siren may also be disarmed when the user logs in to the keypad.

```
AR001 Bell
pgm: --000:00
```

To modify the Bell/Siren PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Bell PGM Pulse ON Time

The bell/siren pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Bell
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Bell PGM Pulse OFF Time

The bell/siren pulse of time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Bell
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Entry Delay PGM or PGM Group

You can assign a entry delay PGM or PGM group to activate whenever the area starts an entry delay cycle. The entry delay PGM or PGM Group will be deactivated when the area is disarmed during the entry delay period or the area activates the alarm due to the entry delay timing out.

```
AR001 Entry
pgm: --000:00
```

To modify the Entry Delay PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Entry Delay PGM Pulse ON Time

The entry delay PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Entry
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Entry Delay PGM Pulse OFF Time

The entry delay PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Entry
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Exit Delay PGM or PGM Group

You can assign an exit delay PGM or PGM group to activate whenever the area starts an exit delay cycle. The exit delay PGM or PGM Group will be deactivated when the area completes the arming cycle or if an alarm occurs during the exit delay period. Disarming the area will also result in the exit delay PGM or PGM group being deactivated.

```
AR001 Exit
pgm: --000:00
```

To modify the Exit Delay PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Exit Delay PGM Pulse ON Time

The exit delay PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Exit
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Exit Delay PGM Pulse OFF Time

The exit delay PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Exit
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Armed PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area completes the arming cycle. The armed PGM or PGM Group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling that the system is armed.

```
AR001 Armed
pgm: --000:00
```

To modify the Armed PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Armed PGM Pulse ON Time

The armed PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Armed
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Armed PGM Pulse OFF Time

The armed PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Armed
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for the pulse output to operate.

Disarmed PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area completes the disarming cycle. The disarmed PGM or PGM Group will be deactivated when the area completes the arming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling that the system is disarmed and can be entered. This can also be used for interlocking non reader controlled doors to prevent entry to areas if the area is armed. Use this output in conjunction with user area's to control multiple storage lockers or storage facilities.

```
AR001 Disarmed
pgm: --000:00
```

To modify the Disarmed PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Disarmed PGM Pulse ON Time

The disarmed PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Disarmed
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Disarmed PGM Pulse OFF Time

The disarmed PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Disarmed
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Bypass PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area has a bypassed zone. The bypass PGM or PGM Group will be deactivated when the area completes the disarming cycle.

```
AR001 Bypass
pgm: --000:00
```

To modify the Bypass PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Bypass PGM Pulse ON Time

The bypass PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Bypass
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Bypass PGM Pulse OFF Time

The bypass PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Bypass
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Tamper PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area has a tamper alarm. The tamper PGM or PGM Group will be deactivated when the area completes the disarming cycle on the 24HR portion of the area.

```
AR001 Tamper
pgm: --000:00
```

To modify the Tamper PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Tamper PGM Pulse ON Time

The tamper PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Tamper
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Tamper PGM Pulse OFF Time

The tamper PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Tamper
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Memory PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area has an alarm and the PGM or PGM group will remain activated. The memory PGM or PGM Group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling that the system has had an alarm activation.

```
AR001 Memory
pgm: --000:00
```

To modify the Memory PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Memory PGM Pulse ON Time

The memory PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Memory
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Memory PGM Pulse OFF Time

The memory PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Memory
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Count PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the user count in an area either reaches 0 or reaches the maximum count (set in the area options). The count PGM or PGM Group will be deactivated depending on the programmed option for the area. Use this option to control car parking and user counting for specific building areas that require limited staff access.

```
AR001 Count
pgm: --000:00
```

To modify the Count PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Count PGM Pulse ON Time

The count PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Count
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Count PGM Pulse OFF Time

The count PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Count
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Defer PGM or PGM Group

You can assign a PGM or PGM group to activate whenever the area begins the defer warning cycle and is about to arm. The defer warning time is programmed in the defer time setting. The defer PGM or PGM Group will be deactivated when the area begins the arming cycle or when the defer time is canceled by a user.

```
AR001 Defer arm
pgm: --000:00
```

To modify the Defer PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Defer PGM Pulse ON Time

The defer PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
AR001 Defer arm
time: 000 on
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Defer PGM Pulse OFF Time

The defer PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
AR001 Defer arm
time: 000 off
```

To modify the pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Defer Arming Warning Time

The defer arming warning time sets the time that the area will warn the user that it is about to arm and that they need to defer the arming (login and press the Disarm Key).

```
AR001 Defer warn
time: 000 off
```

To modify the defer warning time (000 to 255 Minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Defer Keypad Display Group

The defer keypad group is used to display that an area is about to arm on the keypads that belong to the keypad group. The keypads will display this message provided they do not have any higher priority messages that are being displayed. The keypad beeper is recommended to be programmed in the defer PGM output group.

For the Defer Keypad group to generate a message the keypad must also be programmed with the Display Defer Messages.

```
AR001 Defer Grp
None
```

Use the [1] and [3] keys to scroll the keypad group selection and press [ENTER] to select the keypad group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Client Code

The client code for the area is the code that will be used to report alarms to the monitoring station. If the client code is left at the default value of FFFF then the client code that will be used is the client code assigned in the service that is being used to report the alarms.

```
AR001 Client
code: FFFF
```

To modify the client code setting (0000 to FFFF hexadecimal), use the keypad as explained in section Entering Hexadecimal Numbers (see page 335) and press [ENTER].

Lock Door Group on Arming

When programmed this door group will be locked before the arming process starts. This helps to ensure that any door left open zones are closed as the associated doors are locked and the area will be able to arm successfully.

```
AR001 Lock Dr Gp
None
```

Normal Operating Schedule

The normal operating schedule defines the times when the area should be armed and disarmed. This is used to generate the Early/Late to Arm and Disarm Events (see Special Options (see page 127) to enable these events).

```
AR001 Normal Sch
None
```

Period 1 of the schedule defines the time period when the area can be disarmed (Option 5 of the Special Options must be enabled for these events to be generated).

- If the area is disarmed before the start of Period 1 an Early to Disarm event will be generated.
- If the area is still armed when Period 1 ends the System will generate a Late to Disarm event.
- No event is generated is the area is disarmed while Period 1 of the schedule is valid.

Period 2 defines the time period when the area can be armed (Option 6 of the Special Optioning must be enabled for these events to be generated).

- If the area is armed before the start of Period 2 an Early to Arm event will be generated.
- If the area is still disarmed when Period 2 ends the System will generate a Late to Arm event.
- No event is generated is the area is armed while Period 2 of the schedule is valid.

Area Miscellaneous Options

Miscellaneous options for the area include the settings for the restore on bell, child area operations, zone forcing and loiter mode control.

```
AR001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Restore Zones After Bell Time

- Enabled the zones that are assigned to this area will restore when the bell time completes. This does not prevent the zone from generating multiple alarms for another area this setting is specific to the area assigned.

  The zones in the area will still log an event regardless of the bell time to prevent a zone from triggering an event remove the event log option in the zone configuration.

  Setting this option will PREVENT the retrigger bell timer from operating in the zone type, do not use this option for an area that is used for automation control or motion controlled lighting.

- Disabled the zones for the bell will restore each time the zone restores.

Option 2 - Rearm Area If Disarmed

- When enabled the area will re-arm if the area is disarmed. This feature is used for dead man timers and areas that should not remain disarmed for a longer than a predefined time.

  For this option to operate the re-arm time must be set to a value greater than 0.

- Disabled the re-arm operation will not function.

Option 3 - Arm Child Area

- Enabled the child area will be armed when the parent (this) area is armed. Please refer option 4 as this will determine when the area is armed.
- Disabled the child area will not be armed and option 4 will perform no function.

Option 4 - Arm Child Area Only If All Armed

- Enabled the child area will only be armed if ALL the areas that the child area are assigned are armed.

Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.

- Disabled the child area, if option 3 is enabled, will be armed when the parent (this) area arms.

Option 5 - Disarm Child Area

- Enabled the child area will only be disarmed when the parent (this) area disarms.
- Disabled the child area will not be disarmed and option 6 performs no function.

Option 6 - Disarm Child Area Only If All Disarmed

- Enabled the child area will only be disarmed if ALL the areas that the child area are assigned are disarmed.

Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.

- Disabled the child area, if option 5 is enabled, will be disarmed when the parent (this) area arms.

Option 7 - Prevent None Force Zone On Unattended Arming

- Enabled the area will be prevented from arming if a zone that is not a force enabled zone is open when the area is armed in an unattended mode (Software Control, Reader Control or Remote Control).
- Disabled the area will arm regardless of the zone type configuration used.

Option 8 - Area Used For Loiter Control

- Enabled the area will control the users that access the area for a period of time assigned to the loiter control time. If a user breaches the allocated time the user will be set to the area programmed in the loiter area setting.
- Disabled the area does not operate as a loiter area.

Area Reporting Options

Reporting options for the area include the settings for the reporting events and some specific options for the control counting options.

```
AR001 Report
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Closing (Arming) Area

- Enabled the area will generate a reportable event that can be directed to a monitoring station.
- Disabled the area will not generate an event when it is closed (armed).

Option 2 - Report Opening (Disarming) Area

- When enabled the area will generate a reportable event that can be sent to a monitoring station.
- Disabled the area will not generate an event when it is opened (disarmed).

Option 3 - Report Control of the 24HR Tamper Area

- Enabled the area will report both an opening (Disabled) or closing (Enabling) of the 24HR section of this area.
- Disabled the 24HR Tamper Area will not report any enable or disable messages.

Option 4 - Report Bypassed Zones

- Enabled the area will report all zones that are bypassed once it completes the arming process.
- Disabled the area will not report any bypass zones.

Option 5 - User Counting

- Enabled the users that access this area will be counted using the area counting function.
- Disabled the area will not perform any counting.

Option 6 - Arm On Count Reaching 0

- Enabled the area will arm when the count in the area reaches the terminal 0 count.
- Disabled the area will not perform any function on the count reaching 0.

Option 7 - Report Entry Zones Immediately

- Enabled the area will report the activation of an entry zone immediately event though the alarm may be in an entry delay operation.
- Disabled the area will report entry zones if the entry delay times out and the alarm activates.

Option 8 - Clear Area Count On Arming

- Enabled the area will clear the count setting in the area to 0 when the area is armed.
- Disabled the area does not change the count setting when it is armed.

Area Arming Options

Arming options for the area include the settings for the stay, force and instant arming options as well as some count options and banking industry options.

```
AR001 Arming
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Stay Arm

- Enabled the area can be stay armed.
- Disabled the area can not be stay armed.

Option 2 - Force Arm

- Enabled the area can be force armed.
- Disabled the area can not be force armed.

Option 3 - Instant Arm

- Enabled the area can be instant armed.
- Disabled the area can not be instant armed.

Option 4 - Prevent Arming If Trouble Condition

- Enabled the area will be prevented from arming if a trouble condition is present in the system.
- Disabled the area will arm regardless of the trouble condition.

Option 5 - Banking Vault Control Area

- Enabled the area is used to control a vault area.
- Disabled the does not control a vault area.

Option 6 - Banking Vault Dual Control Area

- Enabled the area will require that two users control this area when enabled as a vault control area. This feature will not function unless the area has option 5 enabled.
- Disabled the area will require only one code to control the vault control functions.

Option 7 - Prevent Arming if Count is Not Zero

- Enabled the area will be prevented from arming if the count value for the area is greater than 0.

- Disabled the area will arm regardless of the count value.

Option 8 - Validate Schedule Each Minute

- Enabled the area will verify that the programmed schedule has not changed or the area has not be disarmed when it should be armed. This will occur every one minute period.
- Disabled the area does not check the schedule each minute. If the schedule is programmed the schedule is validated when the start time is reached and when the end time is reached and does not take in to account the control of the area outside these times.

Area Special Options

The special options include a number of specific options that may be required in special circumstances.

```
AR001 Special
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Defer Automatic Arming

- Enabled the area will begin a defer arming cycle prior to starting to arm the area when the area is set to automatically arm on schedule.
- Disabled the area will arm normally.

Option 2 – Force Arm Card Reader

- Enabled the area will force arm the area when the arming process is started by a card reader.
- Disabled the area will arm normally.

Option 3 – Disable Exit PGM on Stay

- Enabled the area will not activate the Exit PGM when the area is stay armed.
- Disabled the area will activate the Exit PGM if programmed when the area is stay armed.

Option 4 – Clear Alarm Memory on Arm

- Enabled the area clear all alarm memory when the area is armed.
- Disabled the area will arm normally.

Option 5 – Early/Late Arm Report

- Enabled the area will generate Early to Arm and Late to Arm reportable events according to the normal operating schedule (see above).
- Disabled the area will not generate these events.

Option 6 – Early/Late Disarm Report

- Enabled the area will generate Early to Disarm and Late to Disarm reportable events according to the normal operating schedule (see above).
- Disabled the area will not generate these events.

Option 7 and 8 – Reserved

- Reserved do not modify

Area Squawk Options

The squawk options determine if the Bell PGM is activated with one short squawk when the system is armed and two short squawks when the system is disarmed.

```
AR001 Special
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Bell Squawk Arm Start

- Enabled the area will squawk the Bell PGM when the arming process starts.
- Disabled the area will not squawk.

Option 2 – Bell Squawk Arm Complete

- Enabled the area will squawk the Bell PGM when the arming process is complete and the exit delay has ended.
- Disabled the area will not squawk.

Option 3 – Bell Squawk Arm Unattended

- Enabled the area will only squawk the Bell PGM when the area is armed by an unattended arming, e.g. Card Reader, Remote Service, Key Switch, Door, another Area etc.
- Disabled the area will not squawk.

Option 4 – Bell Squawk Disarm

- Enabled the area will squawk the Bell PGM when the area is disarmed.
- Disabled the area will not squawk.

Option 5 – Bell Squawk Report OK

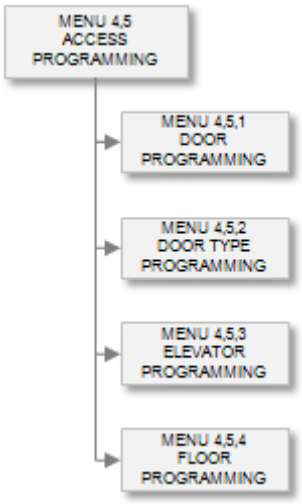
- Enabled the area will squawk the Bell PGM when the a successful Area Armed report has been sent and acknowledge by a reporting service.
- Disabled the area will not squawk.

Options 6,7 and 8 - Reserved

- Reserved do not modify

Access Control

To access the access programming menu, login using a valid code that has access to the access programming menu and then select [MENU, 5]. The Access menu enables you to set up and program all the doors in your system. This includes setting areas outside and inside the door as well as special options for each door.



To allow certain users access to a door the users access level must have a door group assigned. To create or modify door groups refer to the door group programming section. Doors can also be interlocked preventing other users from gaining access to the door if another door is open or not locked.

Door

Each door is assigned a unique door address. Doors are used for the control of access by users or to monitor and control doors to allow the flow of people in to an area.

```
Select door to
modify: DR001
```

To access door programming, login using a valid code that has access to the door programming menu and then select [MENU, 5, 1]. The screen will then prompt you to "Select a door to modify" requesting that you enter a door number. Type the appropriate 3-digit door number or use the [🡻] and [🡹] keys to scroll the available doors. When the desired door number appears on the screen, press [ENTER] to program the selected door. The maximum number of doors that can be programmed is limited by your system's memory and configured profile.

To browse the doors by name press [ENTER] when prompted for a door number to modify and then use the [🡻] and [🡹] keys to scroll the available doors by their name.

Selecting a Door to Modify

Each door is assigned a unique door number from 001 to 250. Your system will be limited to specific number of doors that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Select door to
modify: DR001
```

Type the appropriate 3-digit door number or use the [🡻] and [🡹] keys to scroll the available door numbers. When the desired door number appears on the screen, press [ENTER] to program the selected door number. The maximum number of doors that can be programmed is limited by your system's memory and configured profile.

Door Name

If the selected door has a name associated (some doors do not have a name associated with them) the name programming screen will be shown.

```
DR001 Name

*Door 001
```

To scroll doors by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected door use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the door name will be prefixed by an '*' this indicates that the name is an editable name in the system. Some doors do not have names, this is limited by the system memory and the profile configured.

Door Type Selection

The door type selection allows the door to function in different modes. These modes require the user to present specific credentials for example a card, card and pin, card or pin and pin only. By using a door type these can be scheduled dependent on the time of day allowing different security credentials to be used.

```
DR001 Type
Card Only
```

Use the [1] and [3] keys to scroll the door type selection and press [ENTER] to select the door type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Slave Door

The slave door will follow the primary door (this door) when it unlocks and locks. This can be used to operate a second door that is required to gain access only when a specific entry path is used. For example to gain access to a door a you must access door b.

```
DR001 Slave
None
```

Use the [1] and [3] keys to scroll the slave door selection and press [ENTER] to select the slave door displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Setting a slave door that is the same as the door being programmed will have no affect.

Interlocking Group

The interlocking group is assigned to a door that can not opened or accessed when any of the doors assigned in the interlocking group are not secure. Access will be denied to the user based on an interlock.

```
DR001 Interlock
None
```

Use the [1] and [3] keys to scroll the interlock door group selection and press [ENTER] to select the interlock door group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Inside Area

The inside area defines which area is on the inside of this door. This is used to prevent a user from gaining access to a door when the area is armed and they can not disarm it as well as automatically disarming the area when the door is accessed. Using the door and area control integrates the two systems and is an ideal solution to false alarm prevention.

```
DR001 Inside
None
```

Use the [1] and [3] keys to scroll the inside area selection and press [ENTER] to select the inside area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Outside Area

The outside area defines which area is on the outside of this door. This is used to prevent a user from gaining access to a door when the area is armed and they can not disarm it as well as automatically disarming the area when the door is accessed. Using an inside and an outside area usually requires that the door is programmed with both an entry and exit reader.

```
DR001 Outside
None
```

Use the [1] and [3] keys to scroll the outside area selection and press [ENTER] to select the outside area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Lock Schedule

The lock schedule determines when this door will unlock at a scheduled time. For example an employee entry door may require to be unlocked at 7am and locked at 5pm you would assign a suitable schedule here. Using the unlock on late control option prevents the door unlocking on schedule until the first user access the door.

```
DR001 Lock Sch
None
```

Use the [1] and [3] keys to scroll the unlock schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Unlock Time

The unlock time determines how long the lock that controls the door will remain unlocked for when a user access's the door.

```
DR001 Unlock
time: 005 secs
```

To modify the unlock time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a 000 value will result in the door not unlocking when a users access's the door.

Pre-Alarm Time

The pre-alarm time is programmed to allow the door to be left open for a certain period before it will generate a pre-alarm condition. When the pre-alarm condition is reached this will typically activate a PGM on the PRT-RDI2 that is controlling the door.

```
DR001 Pre-Alarm
time: 030 secs
```

To modify the pre-alarm time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a 000 value will result in the pre-alarm feature not operating.

Maximum Door Open Time

The maximum door open time when it is reached will generate a door left open alarm activating the appropriate trouble zone and PGM output on the PRT-RDI2 that is controlling the door.

The default configuration will mean that the door will generate a left open alarm 15 seconds after the pre-alarm condition. For the trouble zones to activate they must be set in the reader expander.

```
DR001 Max Open
time: 045 secs
```

To modify the maximum door open time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Door Lock PGM or PGM Group

You can assign a PGM or PGM group that controls the physical electric lock for the door. This is typically the lock control PGM on the PRT-RDI2 reader expander that is being used to control the door.

```
DR001 Door Lock
pgm: --000:00
```

To modify the door lock PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Pre Alarm PGM or PGM Group

You can assign a PGM or PGM group that will activate when the pre-alarm time that is programmed is reached. Use this to warn users that the door will generate an alarm if it is left open any longer.

```
DR001 Pre Alarm
pgm: --000:00
```

To modify the pre alarm PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Pre Alarm PGM Pulse ON Time

The pre alarm PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
DR001 Pre Alarm
time: 000 on
```

To modify the pre alarm on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Pre Alarm PGM Pulse OFF Time

The pre alarm PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
DR001 Pre Alarm
time: 000 off
```

To modify the pre alarm pulse off time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Left Open PGM or PGM Group

You can assign a PGM or PGM group that will activate when the maximum open time that is programmed is reached indicating that the door has been left open. Use this to tell users that the door must be closed immediately and that the system has generated an alarm.

```
DR001 Left Open
pgm: --000:00
```

To modify the left open PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Left Open PGM Pulse ON Time

The max open PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
DR001 Left Open
time: 000 on
```

To modify the left open on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Left Open PGM Pulse OFF Time

The left open PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
DR001 Left Open
time: 000 off
```

To modify the left open pulse off time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Forced Open PGM or PGM Group

You can assign a PGM or PGM group that will activate when the door is forced open without any access. Use this feature to activate a local PGM at the door indicating it has been forced.

To generate an alarm on a forced door use the forced door trouble zone and assign this to an area so that a report can be sent to a monitoring station or locally control computer.

```
DR001 Forced
pgm: --000:00
```

To modify the forced open PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Forced Open PGM Pulse ON Time

The forced open PGM pulse on time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.

```
DR001 Forced
time: 000 on
```

To modify the forced open pulse on time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Forced Open PGM Pulse OFF Time

The forced open PGM pulse off time is used to make the PGM output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

```
DR001 Forced
time: 000 off
```

To modify the forced open pulse off time (000 to 255 100ms Increments), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Both the on and off pulse settings must have a value greater than 000 for this feature to operate.

Miscellaneous Options

Miscellaneous options for the door include the control of events that are generated and the function of the door schedule.

```
DR001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Check Schedule Each Minute

- Enabled the door will revalidate the unlock schedule that it is assigned each minute. This will prevent the door from being controlled and locked when it should be unlocked.

  This option also prevents schedule and area control from operating correctly and if enabled will prevent the follow inside and follow outside area status from operating. Setting this option will allow the prevent unlock on arming and normal scheduling operations to occur.

- Disabled the schedule will operate normally and be checked at the start and end times.

Option 2 - Door Open Event When On Schedule

- Enabled the door will not log a door opened event when it is unlocked on schedule. This will prevent the door from filling the event buffer with events that are not needed.
- Disabled the door will generate a door open and close.

Option 3 - Generate Door Pre-Alarm Event

- Enabled the door will generate a pre-alarm event when the pre-alarm timer for the door is reached.
- Disabled no pre-alarm event will be generated.

Option 4 - Generate Door Left Open Event

- Enabled the door will generate a door left open event when the door maximum open time is reached.
- Disabled no left open event will be generated.

Option 5 - Relock Door When Closed

- Enabled the door will lock when it detects a door close event and the lock output is activated.
- Disabled the relock function will not control the door.

Option 6 - Unlock Request To Exit (REX)

- Enabled the door will activate the lock PGM when a request to exit occurs.
- Disabled the door will not control the lock PGM.

Option 7 - Unlock Request To Enter (REN)

- Enabled the door will activate the lock when a request to enter occurs.
- Disabled the door will not control the lock PGM.

Option 8 - Late Open Schedule

- Enabled the Door will not unlock on schedule until the first access has been accepted at the door.
- Disabled the first user in will not prevent the schedule from operating and will activate the door if programmed normally.

Special Options

Special options for the door include the control of the door from the inside and outside areas.

```
DR001 Special
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Door Lock Follows Inside Area

- Enabled the door will unlock if the inside area is disarmed. If no arm/disarm schedule is set, Option 6 MUST be enabled for this function to operate.
- Disabled the door will not unlock when the inside area is disarmed.

Option 2 - Door Lock Follows Outside Area.

- Enabled the door will unlock if the outside area is disarmed. If no arm/disarm schedule is set, Option 6 MUST be enabled for this function to operate.
- Disabled the door will not unlock when the outside area is disarmed.

Option 3 - Prevent Slave Door Unlocking On Inside Area

- Enabled the door will not activate the slave door if the inside area is armed.
- Disabled the slave door will activate regardless of the inside area status.

Option 4 - Prevent Unlock By Schedule If Inside Area Armed

- Enabled the door will not unlock when the schedule is valid if the inside area is armed. Use this option with the late open option to prevent false alarms by entry of personal before an area is disarmed. This option only operates if the option 1 and 2 are not enabled. To prevent unlocking and locking based on schedule and area status set option 6 and 7 to the required values.
- Disabled the door will unlock normally on schedule.

Option 5 - Prevent Unlock By Schedule If Outside Area Armed

- Enabled the door will not unlock when the schedule is valid if the outside area is armed. Use this option with the late open option to prevent false alarms by entry of personal before an area is disarmed.
- Disabled the door will unlock normally on schedule.

Option 6 – Area Disarmed AND Schedule Valid Unlock Door

- Enabled the door will unlock if the door unlock schedule is valid "AND" the inside or outside area is disarmed dependent on the options set for option 4 and 5.
- Disabled the door will perform no AND logic processing for the schedule and area status.

Option 7 - Area Disarmed OR Schedule Valid Unlock Door

- Enabled the door will unlock if the door unlock schedule is valid "OR" the inside or outside area is disarmed dependent on the options set for option 4 and 5.

  If there is no schedule programmed and the door is to follow the area status you must set the OR option to enable the area status to be processed. You also MUST select an inside or outside area.

- Disabled the door will perform no OR logic processing for the schedule and area status.

Option 8 – Generate REX/REN Access Taken Events

- Enabled the door will generate a Request to Exit (or Enter) event if the door opens while the door is unlocked from a request to exit. If the door remains closed an Access Not Taken event will be generated
- Disabled no event will be generated.

Extra Options

Extra options include only the user area control option.

```
DR001 Extra
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Update User Area When Door Has No Anti Pass Back

- Enabled the door will update the users current area even if the door is not programmed with card anti pass back. This can be used to keep track of the user's last area that they entered.
- Disabled the users area will not be modified if the door is not programmed for card anti pass back control.

Option 2 – Prevent Request To Exit If Inside Area Armed

- Enabled the door will deny a request to exit when the inside area has been armed to prevent egress from an armed area.
- Disabled the request to exit operates during any inside area state.

Option 3 – Enable ADA Lock Output

- Enabled the door will multiply the lock output time by two for any user that has been tagged as an ADA (American Disabilities Act) user allowing an extended amount of time for access and door left open.
- Disabled the ADA option has no affect on the door lock time.

Option 4 – Deny Entry if Inside Area Armed

- Enabled the door will deny any entry if the inside area is armed.
- Disabled the inside area will not affect the access decision.

Option 5 – Deny Exit if Outside Area Armed

- Enabled the door will prevent any exit if the outside area is armed.
- Disabled the outside area will not affect the access decision.

Option 6 – Disable Door Open Alarms if unlocked on Schedule, Latch or Area Status

- Enabled the door will not generate the door left open alarm events to the reader expanders beeper and led ports if they are programmed. This allows a door to be "propped" open during normal opening times however a pre-alarm warning will still be generated.

  This option DOES NOT prevent the door left open trouble zone from being sent to the monitoring station if reporting on the trouble zone is programmed to be generated. To prevent the door open alarms from being sent schedule the zone type for the door open alarm events to operate without reporting during the day.

- Disabled the door open alarm events operate normally.

Option 7 – Prompt User Access Type

- Enabled the user will be prompted on the reader expanders associated keypad to enter their reason for access. The user must enter the reason before access will be granted.
- Disabled no prompt will be displayed.

Option 8 - Generate User Access Taken Events

- Enabled the door will generate a User Access Taken event if the door opens while the door is unlocked after entry has been granted. If the door remains closed an Access Not Taken event will be generated.
- Disabled no event will be generated.

Access Time

Typically a door will unlock for a maximum of 5 seconds. Some users, especially the physically impaired, may find this time too short so it is possible to extend the door access time by entering a value into the Door Extended Access Time box. The value entered is in seconds. The door will unlock for the specified time only if the User who accesses the door is configured as an Extended Access user (configured under the Users options).

```
DR001 Extnd Axs
time: 00005 secs
```

To modify the Extended Access time (00001 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Timed Anti-passback

If the Door Type assigned to the Door has anti-passback enabled then the door can have a specific anti-passback time assigned for Entry and another time for Exit. When a user uses the door for Entry or for Exit the time period begins and the user will not be granted repeat access to the door until the time has expired. The time is set in minutes. This function is qualified by the global flag *Enable Timed User Anti-Passback Reset* which is set under the Panel properties/Options settings.

```
DR001 PassEntry
time: 65535 mins

DR001 PassExit
time: 65535 mins
```

To modify the Pass Entry and Pass Exit time (00001 to 65534 minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. A value of 65535 will disable this function.

Door Type

Each door type is assigned a unique door type address. There are four default door types that will cover nearly all the configurable options. To access door type programming, login using a valid code that has access to the door type programming menu and then select [MENU, 5, 2]. The screen will then prompt you to "Select a door type to modify" requesting that you enter a door type number. Type the appropriate 3-digit door type number or use the [🡻] and [🡹] keys to scroll the available door types.

```
Door type to
modify: DT001
```

When the desired door type number appears on the screen, press [ENTER] to program the selected door type. The maximum number of door types that can be programmed is limited by your system's memory and configured profile.

To browse the door types by name press [ENTER] when prompted for a door type number to modify and then use the [🡻] and [🡹] keys to scroll the available door types by their name.

Selecting a Door Type to Modify

Each door type is assigned a unique door type number from 001 to 064. Your system will be limited to specific number of door types that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Door type to
modify: DT001
```

Type the appropriate 3-digit door type number or use the [🡻] and [🡹] keys to scroll the available door type numbers. When the desired door type number appears on the screen, press [ENTER] to program the selected door type number. The maximum number of door types that can be programmed is limited by your system's memory and configured profile.

It is recommended NOT to modify the door types DT001 to DT004. These are assigned by default to all doors. When scheduling door type operation or altering default settings use the door types from DT005 and above.

Door Type Name

If the selected door type has a name associated (some door types do not have a name associated with them) the name programming screen will be shown.

```
DT001 Name
Card Only
```

To scroll door types by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected door type use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the door type name will be prefixed by an '*' this indicates that the name is an editable name in the system. Some door types do not have names, this is limited by the system memory and the profile configured.

Operational Schedule

The door type schedule allows a door type to be scheduled for use during a certain time period. For example setting a door type schedule for card only from between 9am and 5pm and then a secondary door type of Card and Pin will mean during the hours of 9am and 5pm any door assigned the door type will require card only access during 9am and 5pm however outside this time will require a card access and pin number. Use this option to increase the security of the main entry doors after hours while maintaining a faster traffic flow during working hours.

```
DT001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

If a schedule is selected and no secondary door type is programmed all doors that are assigned this door type will not function when the schedule becomes invalid.

Secondary Door Type

The secondary door type is used in conjunction with the schedule to allow a door to have a secondary configuration when the schedule that is assigned is invalid. This allows different modes of control over the method a user access the door. For example between 8am and 12pm the user can be required to access the door with only a card however outside these hours a card and pin is required.

```
DT001 Schedule
None
```

Use the [1] and [3] keys to scroll the secondary door type selection and press [ENTER] to select the door type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Entry Operation Mode

The reader entry operation mode determines how an entry reader that is associated with the door that has this door type assigned will operate. There are four possible modes that can be set to allow the use of card, card and pin, card or pin and pin only to operate.

```
DT001 Read In
Card Only
```

Use the [1] and [3] keys to scroll the reader in modes and press [ENTER] to select the mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Anti Pass Back Entry Operation Mode

The reader anti pass back operation mode determines how an entry reader controls the ability for a user to pass back their card or details for another person to gain access while they are already inside a protected area. The Protege System use's global anti pass back per controller.

Selecting soft pass back will allow the user entry however it will log an error in the buffer that a pass back violation has occurred. Selecting hard pass back will prevent the user from gaining entry and also log an event.

```
DT001 Pass In
None
```

Use the [1] and [3] keys to scroll the anti pass back modes and press [ENTER] to select the mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Exit Operation Mode

The reader in operation mode determines how an exit reader that is associated with the door that has this door type assigned will operate. There are four possible modes that can be set to allow the use of card, card and pin, card or pin and pin only to operate.

```
DT001 Read Out
Card Only
```

Use the [1] and [3] keys to scroll the reader in modes and press [ENTER] to select the mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Anti Pass Back Exit Operation Mode

The reader anti pass back operation mode determines how an exit reader controls the ability for a user to pass back their card or details for another person to gain access while they are already inside a protected area. The Protege System use's global anti pass back per controller.

Selecting soft pass back will allow the user to exit however it will log an error in the buffer that a pass back violation has occurred. Selecting hard pass back will prevent the user from exiting the area and also log an event.

```
DT001 Pass Out
None
```

Use the [1] and [3] keys to scroll the anti pass back modes and press [ENTER] to select the mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Entry Options

Entry options for the door type are currently all reserved and perform no function.

```
DT001 Entry
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1, 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Exit Options

Exit options for the door type are currently all reserved and perform no function.

```
DT001 Exit
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1, 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Miscellaneous Options

Miscellaneous options for the door type are used to control the REX and REN operation of the door. Use these settings to prevent the request to exit and request to enter from operating when an area is armed or when a function is being processed.

```
DT001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Disable REX Request To Exit

- Enabled the door will disable the REX (request to exit) operation.
- Disabled the door will allow REX (request to exit) operation.

Option 2 – Disable REN Request To Enter

- Enabled the door will disable the REN (request to enter) operation.
- Disabled the door will allow REN (request to enter) operation.

Option 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Elevator

Each elevator is assigned a unique elevator address. Elevators are used for the control of access by users or to monitor and control floors in a multi story high rise buildings.

```
Elevator to
modify: EL001
```

To access elevator programming, login using a valid code that has access to the elevator programming menu and then select [MENU, 4, 5, 3]. The screen will then prompt you to "Select a Elevator to modify" requesting that you enter a elevator number. Type the appropriate 3-digit elevator number or use the [🡻] and [🡹] keys to scroll the available elevators. When the desired elevator number appears on the screen, press [ENTER] to program the selected elevator. The maximum number of elevators that can be programmed is limited by your system's memory and configured profile.

To browse the elevators by name press [ENTER] when prompted for a elevator number to modify and then use the [🡻] and [🡹] keys to scroll the available elevators by their name.

Selecting an Elevator to Modify

Each elevator is assigned a unique door number from 001 to 250. Your system will be limited to specific number of elevators that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Elevator to
modify: EL001
```

Type the appropriate 3-digit elevator number or use the [🡻] and [🡹] keys to scroll the available elevator numbers. When the desired elevator number appears on the screen, press [ENTER] to program the selected elevator number. The maximum number of elevators that can be programmed is limited by your system's memory and configured profile.

Elevator Name

If the selected elevator has a name associated (some elevators do not have a name associated with them) the name programming screen will be shown.

```
EL001 Name
*Elevator 001
```

To scroll elevators by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected elevator use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the elevator name will be prefixed by an '*' this indicates that the name is an editable name in the system. Some elevators do not have names, this is limited by the system memory and the profile configured.

General Options

General options configure the elevator for various operational modes and functions.

```
EL001 General
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Destination Reporting Mode Enabled

- Enabled the elevator will operate in DRM mode allowing only one button to be selected by the user when the present their card.

When using the DRM mode the PRT-PX16 modules that are used for elevator control must have a PRT-PX16-DRI board attached to allow the connection of button feedback inputs.

- Disabled the elevator will operate in normal mode with one badge activating the appropriate floor relays for the user.

Option 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Reader Expander

The reader expander selection programs the elevator to send the activation of floor information and floor selection to the reader expander programmed. You must also set the port number in the next screen to the appropriate port driving this elevator.

```
EL001 Reader
None
```

Use the [1] and [3] keys to scroll the reader expanders that are available and press [ENTER] to select the expander displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reader Port

The reader port selection programs the elevator to communicate on this port with the expander number selected above. You must also set the reader expander number in the previous screen.

```
EL001 Port
None
```

Use the [1] and [3] keys to scroll the reader port and press [ENTER] to select the port displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Floor Open Time

The floor open time configures the amount of time that a floor will be activated for when it has been selected or the amount of time the floor relay will be activated for when the user has presented a card.

```
EL001 Open
time: 005 secs
```

To modify the Floor open time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Destination Select Time

The destination select time configures the amount of time that user has to select a floor when they present their card.

```
EL001 Select
time: 005 secs
```

To modify the floor select time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Floor Configuration

Each floor in an elevator can be assigned options, an unlock schedule and an area. These options configure how the floor will function. You must select the floor to modify for the elevator that you are programming.

```
EL001 Floor to
modify: FL001
```

Type the appropriate 3-digit floor number or use the [🡻] and [🡹] keys to scroll the available floors for the elevator. When the desired floor number appears on the screen, press [ENTER] to program the selected floor.

Floor Operation Schedule

The floor operation schedule can be assigned to each floor allowing the floor to unlock at the programmed times within the schedule. A schedule is valid when the time of day falls between any start and end time provided the day of the week is selected and holidays are not affecting the schedule. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
FL001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

A schedule selection of NONE will disable the floor unlock schedule and no action will be taken on the floor.

Floor Area

The floor area defines which area is on the inside of this floor. This is used to prevent a user from gaining access to a floor when the area is armed and they can not disarm it as well as automatically disarming the area when the floor is accessed. Using the floor and area control integrates the two systems and is an ideal solution for false alarm prevention.

```
FL001 Area
None
```

Use the [1] and [3] keys to scroll the floor area selection and press [ENTER] to select the floor area displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

General Options

General options configure the floor for various operational modes and functions.

```
EL001 General
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Unlock Elevator Floor Late To Open

- Enabled the floor will only be unlocked on schedule if a valid access has been made to the selected floor.

Unlock late to open will only operate if the elevator is configured for destination reporting and a PRT-PX16-DRI is present.

- Disabled the floor will follow the floor schedule if programmed.

Option 2 – Validate Schedule Every Minute

- Enabled the floor state will be checked against the schedule every minute and change state accordingly.
- Disabled the floor will unlock at the start time of the schedule and lock at the end time. The floor will not be controlled during this time by the schedule.

Option 3 – Follow Area Status

- Enabled the floor will follow the status of the area. If the area is armed the floor will lock and if the area is disarmed the floor will unlock.
- Disabled the floor will not follow the area status.

Option 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Floor

Each floor is assigned a unique floor number in the Protege System. Each elevator can have a maximum of 128 floors. Floors are given a name that is used when generating events and reporting information.

```
Floor to
modify: FL001
```

To access elevator programming, login using a valid code that has access to the floor programming menu and then select [MENU, 4, 5, 3]. The screen will then prompt you to "Select a Floor to modify" requesting that you enter a floor number. Type the appropriate 3-digit floor number or use the [🡻] and [🡹] keys to scroll the available floors. When the desired floor number appears on the screen, press [ENTER] to program the selected floor. The maximum number of floors that can be programmed is limited by your system's memory and configured profile.

To browse the floors by name press [ENTER] when prompted for a floor number to modify and then use the [🡻] and [🡹] keys to scroll the available floors by their name.

Selecting a Floor to Modify

Each floor is assigned a unique door number from 001 to 250. Your system will be limited to specific number of floors that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Floor to
modify: FL001
```

Type the appropriate 3-digit floor number or use the [🡻] and [🡹] keys to scroll the available floor numbers. When the desired floor number appears on the screen, press [ENTER] to program the selected floor number. The maximum number of floors that can be programmed is limited by your system's memory and configured profile.

Floor Name

If the selected floor has a name associated the name programming screen will be shown.

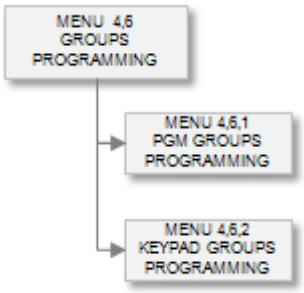
```
FL001 Name
*Floor 001
```

To scroll floors by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected floor use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the floor name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Group

Groups of objects allow you to control multiple objects in the Protege System. Groups include PGM and Keypad Groups. To go to the groups sub menu select [MENU, 4, 6]. You can then select from the PGM Group or Keypad Group menu or scroll the menu using the [↑] and [↓] keys.



PGM Group

To access the PGM group programming login using a valid installer code and then select [MENU, 4, 6, 2]. The screen displays "PGM Group to modify" as shown in the following example.

PGM groups allow you to control multiple PGM outputs from one PGM entry point selection in the Protege System. When you assign a PGM or a PGM group to a module or an area, for example, the screen displays the PGM address format by default.

```
PGM Group to
modify: PG001
```

When the desired PGM group appears on the screen, press [ENTER] to program the PGM group. The maximum number of PGM groups that can be programmed is limited by your system's memory and configured profile.

To browse the PGM groups by name press [ENTER] when prompted for a PGM group to modify and then use the [↓] and [↑] keys to scroll the available PGM groups by their name.

Selecting a PGM Group to Modify

Each PGM Group is assigned a unique door type number from 001 to 064. Your system will be limited to specific number of PGM groups that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
PGM Group to
modify: PG001
```

Type the appropriate 3-digit PGM group number or use the [↓] and [↑] keys to scroll the available PGM groups. When the desired PGM group appears on the screen, press [ENTER] to program the selected PGM Group.

PGM Number 1 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 1 of 8 in this location.

```
PG001 Item [1]
pgm: --000:00
```

To modify the PGM item 1 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 2 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 2 of 8 in this location.

```
PG001 Item [2]
pgm: --000:00
```

To modify the PGM item 2 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 3 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 3 of 8 in this location.

```
PG001 Item [3]
pgm: --000:00
```

To modify the PGM item 3 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 4 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 4 of 8 in this location.

```
PG001 Item [4]
pgm: --000:00
```

To modify the PGM item 4 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 5 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 5 of 8 in this location.

```
PG001 Item [5]
pgm: --000:00
```

To modify the PGM item 5 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 6 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 6 of 8 in this location.

```
PG001 Item [6]
pgm: --000:00
```

To modify the PGM item 6 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 7 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 7 of 8 in this location.

```
PG001 Item [7]
pgm: --000:00
```

To modify the PGM item 7 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

PGM Number 8 In PGM Group

Each PGM group can be assigned up to 8 PGM's program the item number 8 of 8 in this location.

```
PG001 Item [8]
pgm: --000:00
```

To modify the PGM item 8 entry, use the settings as explained in section Entering PGM and PGM Groups (see page 336). You can not program a PGM group that will reference a PGM group in the PGM item settings.

Keypad Group

To access the keypad group programming login using a valid installer code and then select [MENU, 4, 6, 2]. The screen displays "keypad Group to modify" as shown in the following example.

```
Keypad group to
modify: KG001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the area groups in the Protege System allow you to configure how a user will interact with the areas in the system and what areas they are able to access.

Selecting a Keypad Group to Modify

Each keypad group is assigned a unique keypad group number from 001 to 250.

```
Keypad Group to
modify: KG001
```

Type the appropriate 3-digit keypad group number or use the [🡻] and [🡹] keys to scroll the available keypad groups. When the desired keypad group number appears on the screen, press [ENTER] to program the selected keypad group. The maximum number of keypad groups that can be programmed is limited by your system's memory and configured profile.

Keypad Group Name

If the selected area group has a name associated (some area groups do not have a name associated with them) the name programming screen will be shown.

```
KG001 Name
All Keypads
```

To scroll keypad groups by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected keypad group use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the keypad group name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the keypad group determines when the keypad group is valid and if it will use a secondary keypad group if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

```
KG001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Keypad Group

A secondary keypad group can be selected that will be used when the schedule of the keypad group that is being programmed is not valid. The schedule of the secondary area group must be valid or set to none.

```
KG001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary keypad group selection and press [ENTER] to select the keypad group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary keypad group that uses the current keypad group being edited will perform no function.

Keypad Group Assignment Blocks 1 to 32

The keypad group assignment blocks assign a keypad to the group that is being programmed. Each block is 8 keypads and the number of keypad blocks depends on the number of keypads that the system is configured to manage. For example if there are 16 keypads there will be 2 blocks of 8 keypads. Block 1 option 1 will refer to Keypad 001 and Block 2 Option 8 will refer to Keypad 016.

```
KG001 Block 1
   [12345678]
```

To modify the block setting options, follow the settings as explained in section Entering Data Options (see page 336). Use the relevant key from 1 to 8 to toggle the state of the option.

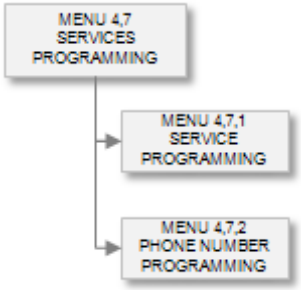
Pressing the [ENTER] key will move you to the next block in the keypad group until you return to the keypad group selection.

The following table shows the relationship between the block and the keypad that is being selected for the keypad group. For example if you want to select keypad 023 you would go to block 3 and then change the 7 option.

Block #	Opt 1	Opt 2	Opt 3	Opt 4	Opt 5	Opt 6	Opt 7	Opt 8
1	KP 001	KP 002	KP 003	KP 004	KP 005	KP 006	KP 007	KP 008
2	KP 009	KP 010	KP 011	KP 012	KP 013	KP 014	KP 015	KP 016
3	KP 017	KP 018	KP 019	KP 020	KP 021	KP 022	KP 023	KP 024
4	KP 025	KP 026	KP 027	KP 028	KP 029	KP 030	KP 031	KP 032
5	KP 033	KP 034	KP 035	KP 036	KP 037	KP 038	KP 039	KP 040
6	KP 041	KP 042	KP 043	KP 044	KP 045	KP 046	KP 047	KP 048
7	KP 049	KP 050	KP 051	KP 052	KP 053	KP 054	KP 055	KP 056
8	KP 057	KP 058	KP 059	KP 060	KP 061	KP 062	KP 063	KP 064

Reporting

The reporting of messages and control of communication services is done from within the reporting menu. The reporting menu allows the programming of services for communication to central station monitoring systems, offsite ModBUS communication receivers, local computer monitoring using the PRT-SMGT Protege System Management Suite and dial up communication.



To go to the reporting menu select [MENU, 4, 7]. You can then select from the menu items presented or scroll the menu using the [🡅] and [🡇] keys.

Services

To access the communication service programming menu login using a valid installer code and then select [MENU, 4, 7, 1]. The screen displays "Service to modify" as shown in the following example.

```
Service to
modify: SV001
```

Services are a vital component to the Protege System and allow many communication and monitoring functions to be performed. Services are small independent functions within the Protege that are used to communicate information or perform specialized control functions. An example of a communication service that is programmed by default for SV001 is the local PC computer upload service.

When the service appears on the screen, press [ENTER] to program the service. The maximum number of services that can be programmed is limited by your system's memory and configured profile.

Services that dial telephone numbers to report or send information to a remote location may be limited by a fixed maximum number of dialing attempts. This configuration limitation only applies in countries that impose a dialing attempts restriction and only settings below this value are allowed. Please verify with your local communications regulatory agency if you are not familiar with the dialing configuration for your region.

Selecting a Service to Modify

Each service is assigned a unique service number from 001 to 016. Your system will be limited to specific number of services that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Service to
modify: SV001
```

Type the appropriate 3-digit service number or use the [🡇] and [🡅] keys to scroll the available services. When the desired service appears on the screen, press [ENTER] to program and control the selected service.

Controlling Services (Starting and Stopping)

For a service to start performing the function that it is programmed for you must start the service. This is achieved by using the [1] key to start a service and the [2] key to stop a service.

If the service is running when you selected it to program a message will be displayed to indicate the service is locked and can only be viewed. To edit the service you must press the [2] key to stop the service, wait for the display to show the halted message and then proceed with programming.

```
SV001 State
Halted
```

If the service is running and changes are made to the service the system will not save these to the programmed service.

Type Of Service

The type of service that is programmed will determine the operation that this service will perform. This will also determine the programming screens that follow in each of the sub sections as the programming of services can contain many features and options dependent on this selection.

```
SV001 Ser Type
None
```

Use the [1] and [3] keys to scroll the service types and press [ENTER] to select the service type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The following table includes a complete explanation of each service type that is programmable in the Protege System. Services require the use of onboard hardware devices or expansion devices.

Service Type	Function
None	The service will perform no function and control no hardware resources. This service can not be started or halted.
Automation Control Service	Provides a generic interface for integration with third party automation products such as those provided by Control 4, Crestron, AMX, C-Gate and Command Fusion
BACnet	Enables external devices to monitor and control the state of PGMs on the Protege system.
C-Bus	Provides integration with building control and automation products using the Clipsal C-Bus protocol.
Contact ID	Sends alarms, tests and events using the Contact ID reporting format to a monitoring station capable of receiving the Contact ID format. This service will share the modem with the SIA, Monitor Phone and ModBUS remote services if they are running.
DVAC	Used to report over the DVAC hard line communication link using the Surgard Receiver protocol. Reports alarms, test and activity in the system. Monitors locally the polling and link status. The availability of a DVAC hard line is dependent on the location of the installation.
GSM Modem	Enables the Protege System controller to send alarm and activation information via SMS messaging
Intercom	Provides a direct link to intercom solutions, allowing automatic token generation for elevators, doors and control functions
Link Me	Provides an interface for Protege System Controllers to communicate together through the linking of PGM outputs. This service maps PGMs on one System Controller to a second System Controller so they follow the state of the primary System Controller.
ModBUS	The ModBUS slave protocol allows the communication and control of objects (Zones, Areas, PGM's, Doors etc.) from a standard industrial automation package such as Citect, Wonderware, The FIX and DAQ Factory. There are many other products that support the ModBUS protocol and will communicate with the Protege System.

Service Type	Function
ModBUS (Remote)	The ModBUS remote protocol communicates with a remote Protege System using intelligent on-demand reporting for large scale, wide area monitoring using a standard SCADA package while adding the ability to protect and control access to the remote outstation.
Monitor Phone	Monitors the onboard modem for incoming upload/download connections, performs line fault monitoring and pc callback functions. This service will share the modem with the Contact ID, SIA and ModBUS Remote and other services that use the onboard modem if they are running.
Report IP	Allows the Protege System controller to send alarm and activation information over an IP connected network. The Report IP Service supports multiple formats and allows the connection to third party reporting if required.
Serial Printer	Prints events to a standard serial communication port. Can be programmed to only print specific event groups or events from a specific area. Option to send Hexadecimal Events and PC acknowledgement functions for use with Third Party OEM event retrieval systems.
SIA	Sends alarms, tests and events using the SIA Level 2 reporting format to a monitoring station capable of receiving the SIA Level 2 format. This service shares the modem with the Contact ID, Monitor Phone and ModBUS remote services if they are running.
Upload Direct	Provides the interface between the System Controller and the Protege System Management Suite Software. This service must always be present.
Viz IP	Provides an interface for Protege System Controllers to communicate to a DVR over IP that has the VizIP IP communication protocol. This service maps PGMs on the System Controller to the alarm outputs from the DVR, eliminating the need to have physical wiring connections from the DVR to the Protege System Controller.

The services require specific programming for the type that is selected, the following details the programming information for each service type.

Contact ID Reporting Service

To program the contact ID reporting service ensure that the service you have selected it halted. Select the service type selection screen as shown below for Contact ID.

```
SV001 Ser Type
Contact ID
```

Use the [1] and [3] keys to scroll the service types until you reach the contact ID selection and press [ENTER] to select the contact id service type displayed and proceed to the next programmable option for the contact ID service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to Start With The Operating System (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. To only start and stop the service manually select the manual option.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Contact ID Client Code

The contact ID client code is used to identify the system to the remote monitoring company when a report is generated. The client code will accept hexadecimal numbers however this will be dependent on the ability of the receiver and should be verified before configuration.

```
SV001 Client
code: 0000
```

Type the appropriate 4 digit client code, after each digit you must press [←] and [➔] to move to the next digit. When the desired client code is entered, press [ENTER] to save the programmed setting and move to the next screen. For more information about hexadecimal data entry refer to the section Hexadecimal Data Entry (see page 335).

PABX Phone Number

The PABX phone number is dialed to gain an outside line if the system is connected to a internal phone extension. The PABX phone number can also be programmed with a schedule in the case that between certain times the phone line is directly connected with an outside line.

```
SV001 PABX
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Phone Number One

The primary phone number will be dialed by the contact ID service when it first is initiated to report an event. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).

```
SV001 Phone 1
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Phone Number Two

The secondary phone number will be dialed by the contact ID service if a connection with the central station can not be made on the primary phone number. This may be dialled after the total number of attempts is reached on the primary or sequential until the total number of attempts is reached for the primary and secondary numbers. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).

```
SV001 Phone 2
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Backup Phone Number

The backup phone number will be dialed by the contact ID service if a connection with the central station can not be made on either the primary or secondary phone number. This will be dialled after the total number of attempts is reached on the primary and secondary numbers. The backup number will be dialled for the configured number of dialing attempts programmed for the service. For information on the dialing sequence refer to the section Sequential Dialing Attempt (see page 198) and Alternate Dialing Attempts (see page 199).

```
SV001 Backup
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Dial Options

The dial options configure the service as to how it is meant to dial when a reportable event has been generated.

```
SV001 Dial
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Alternate Dialing Configuration

- Enabled the dialer will use the alternate dialing method, refer to the Alternate Dialing section (see page 199).
- Disabled the dialer will use sequential dialing method, refer to the Sequential Dialing section (see page 198).

Option 2 - DTMF Tone / Pulse Dialing

- Enabled the dialer will use pulse dialing to dial out.
- Disabled the dialer will always use DTMF to dial except when Option 3 has been enabled.

Option 3 - Switch Dialing To Pulse On 5th Attempt

- Enabled the dialer will switch to the pulse dialing format on the 5th attempt to dial the selected phone number.
- Disabled the dialer will always use DTMF to dial.

Option 4 - Switch To Second Phone Line On Failure

- Enabled the dialer will switch the secondary phone line over and use this to dial if the first phone line fails or fails to communicate.
- Disabled the dialer will use the first phone line.

Option 5 - PABX Requires Pause

- Enabled the dialer will insert a pause of 2.5 seconds after the PABX telephone number is dialled.
- Disabled the dialer will dial the numbers with a standard DTMF inter digit delay.

Option 6, 7 and 8 - Reserved

- Reserved do not modify

Events Options

The events options allow you to filter the type of events that this contact ID service will send to the monitoring station.

```
SV001 Events
   [123456--]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Opens

- Enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report opens.

Option 2 - Report Closes

- Enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report closes.

Option 3 - Report Alarms

- Enabled the service will report alarms for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report alarms.

Option 4 - Report Tampers

- Enabled the service will report tampers for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report tampers.

Option 5 - Report Restore

- Enabled the service will report restores for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report restores.

Option 6 - Report Bypass

- Enabled the service will report bypass's for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report bypass's.

Option 7 and 8 - Reserved

- Reserved do not modify

Data Options

The data options are currently reserved and should not be modified from their default settings.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Service Used For Back Up Operation

- Enabled the service will NOT report messages and alarms unless it is started by another service that has failed. It will then start reporting messages immediately from the point that the service that started it failed to report and then return operation to the service that started. This cycle will continue until the service that failed operates normally.

When using a service in Back Up mode the service should be programmed with the same area group and account code as the service it is backing up. In some cases it may be desirable to program a different account code for the back up service. Consult with your Monitoring Station Operator to ensure you correctly configure the back up service.

- Disabled the dialer will operate as a normal service and report alarms as programmed.

Option 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Miscellaneous Options

The miscellaneous options allow you to program special functions and features for the contact ID service.

```
SV001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Modem Service Events

- Enabled the service will provide step by step event information showing the call progression and detailed logging information. This option can be turned on for diagnostic purposes but should not be enabled as large volumes of events are stored.
- Disabled the dialer will not log events.

Option 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Area Group

An area group will define which areas this service will process when a reportable event is generated. An area group of None (default) will result in all areas being sent with the service.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reporting Table

With the size of the Protege system the maximum reporting points available in the Contact ID format is easily exceeded, to allow flexibility a reporting table has been created to allow information to be sent using pre-defined zone numbers or values. There are 2 predefined configurations for the reporting tables and 8 custom tables that can be configured for use by any of the services. For information on the custom tables refer to the Table Configuration section (see page 282).

```
SV001 Reporting
Table 000
```

Use the [1] and [3] keys to scroll the reporting tables selection and press [ENTER] to select the reporting table displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Dialing Attempts

The dialing attempts determine how many times the dialer will attempt to dial a number before failure. This setting will be overridden by the modem configuration dependent on the country of installation. For UL and ULC installations this value can not be set above 8 and will be internally restricted if a value is programmed above this value. The dialing attempts operates in conjunction with the dialing delay setting.

```
SV001 Dialing
attempts: 008
```

To modify the dialing attempts (000 to 255, a setting of 000 will result in the default of 8 attempts being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Port Open Attempts

The port open attempts determine how many times the service will wait for the modem to become available if another service is already using modem for communication. This operates in conjunction with the port open time settings.

```
SV001 Port open
attempts: 008
```

To modify the port open attempts (000 to 255, a setting of 000 will result in the default of 8 port attempts being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Report Count

The report count if set to a value other than 000 will restrict the service from sending more than the programmed number of reports to the monitoring station. When using multiple reporting paths that potentially can report the same event to 2 or more locations the report count should be programmed with an acceptable limit (Between 8 and 16 is recommended).

```
SV001 Report
count: 000
```

To modify the report count (000 to 255, a setting of 000 will result in an unlimited number of reports being able to be sent), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Handshake Time

The handshake time determines the time it takes for the remote receiving unit to answer and provide a handshake message for the contact ID format. By default this is set to 030 seconds and should only be adjust if a longer than normal call completion is required.

```
SV001 Handshake
time: 030
```

To modify the handshake time (000 to 255, a setting below 010 will result in the default of 30 seconds being programmed), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Redial Time

The redial time determines inter phone number dialing timeout. A value of 20 seconds is programmed by default meaning each phone number will be dialled with 20 second intervals from the time the previous call was terminated.

```
SV001 Redial
time: 020
```

To modify the redial time (000 to 255, a setting below 010 will result in the default value of 030 being programmed), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Off Hook PGM

The off hook PGM is activated when the service takes the telephone line and is deactivated when the service completes communication. This PGM setting can be used with remote exchange systems that require ground start communication connections.

```
SV001 Off Hook
pgm: --000:00
```

To modify the off hook PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Report OK PGM

The report ok PGM is activated when the service completes the reporting and the messages have been successfully acknowledge. The PGM is activated when the service returns a reporting complete result OK message. The PGM is not deactivated and should be programmed with a timer, this can be connected to an external audible device to signal that the report was completed. Using this feature with the shorten exit delay for an area allows an end user to verify the communication path on arming of the building

```
SV001 Report Ok
pgm: --000:00
```

To modify the report ok PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Monitor Phone Service

To program the monitor phone service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
Monitor Phone
```

Use the [1] and [3] keys to scroll the service types until you reach the monitor phone selection and press [ENTER] to select the monitor phone service type displayed and proceed to the next programmable option for the monitor phone service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to Start With The Operating System (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. To stop and start the service manually and to prevent the service from restarting when a reset condition occurs select manual operation.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Miscellaneous Options

The miscellaneous options allow you to program special functions and features for the monitor phone service.

```
SV001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Telephone Line Monitoring

- Enabled the service monitor the telephone line for a disconnection or out of tolerance loop value. The TLM failure will open the phone line trouble zone, for a list of trouble zones refer to the Trouble Zone section (see page 94).

  Only telephone line 1 (T1 and R1) can be monitored for telephone line or loop failures.
- Disabled the service will not monitor the telephone line.

Option 2 - Answer Machine Override

- Enabled the service will use the answer/fax machine override function.
- Disabled the service will answer the line based on the programmed number of rings to answer.

Option 3 - Call Back Security On Connection Request

- Enabled the service will allow a remote communication connection to login and will then call the connecting party back using the PC phone number programmed in the service.
- Disabled the service will not use call back security.

Option 4 - Call Back On Event Buffer (75%)

- Enabled the service will call the PC phone number programmed in the service when the total number of events that have not been enabled reaches 75% of the total available events.
- Disabled the service will not call back.

Option 5 - Log Modem Service Events

- Enabled the service will provide step by step event information showing the call progression and detailed logging information. This option can be turned on for diagnostic purposes but should not be enabled as large volumes of events are stored.
- Disabled the dialer will not log events.

Option 6 - Reserved

- Reserved do not modify

Option 7 - Reserved

- Reserved do not modify

Option 8 - Answer ModBUS Remote Receiver Mode

- Enabled the service will answer the phone line and wait for a ModBUS remote communication connection. Setting this option will disable the ability to log in to the panel using the Protege System Management Suite. This option should only be enabled for the ModBUS remote receiver unit. For information on the ModBUS remote communication operation refer to the PRT-CTRL ModBUS Remote and Slave Communication Protocol Reference Manual.
- Disabled the dialer will answer using the normal configuration settings.

Answering Machine Override Delay Time

The answering machine override setting determines the delay between the first group of rings that are generated to the time that the panel will immediately hook and take the line in answer mode. The number of rings must be less than 10 seconds and then the call back must occur within 30 seconds (default) of the initial rings. The answer machine override option must be enabled for the operation to work.

```
SV001 AMO Delay
time: 030 secs
```

To modify the answer machine override delay (000 to 255, a setting of 000 will result in the default of 030 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Carrier Delay Time

The carrier delay time is used when the service is performing a dial out to a remote computer or system. The carrier delay time determines how long the service will wait for a carrier and connection to be made with the remote system. The time set should include in call progression and rings to answer time for the remote system and any variance in these times. For example for a remote call, it takes 10 seconds and then the modem takes 5 seconds to answer and 5 seconds to generate the required carrier, it is therefore recommended to set this value to between 35 and 40 seconds, this covers any variation in these times.

```
SV001 Carrier
time: 030 secs
```

To modify the carrier delay time (000 to 255, a setting of 000 will result in the default of 030 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Call Host Attempts

The call host attempts set the number of times the service will attempt to call the host PC Phone number before giving up. This applies to all outgoing communication with a remote computer (Event Call and Call Back Security On Login).

```
SV001 Call host
attempts: 008
```

To modify the call host attempts (000 to 255, a setting of 000 will result in the default of 008 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Rings To Answer

The rings to answer sets the number of rings the modem will wait before taking the line and generating carrier.

```
SV001 Rings to
answer: 008
```

To modify the rings to answer (000 to 255, a setting of 000 will result in the modem not answering the line), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

PC Phone Number

The PC or remote phone number will be dialed by service when the Call Back Security Connection option is enabled and a call back event is required or when the automatic event upload option is enabled. In both cases the PC phone number is dialled sequentially for the maximum dialing attempts programmed in the service.

```
SV001 Phone 1
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Protege SMGT Service

To program the Protege SMGT service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen. By default the Protege SMGT service is programmed at SV001 and is running using the programmed TCP/IP address and port 10000.

```
SV001 Ser Type
Protege SMGT
```

Use the [1] and [3] keys to scroll the service types until you reach the Protege SMGT selection and press [ENTER] to select the Protege direct service type displayed and proceed to the next programmable option for the Protege direct service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode 1

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communication Port

The communication port defines the interface that this service will use to communicate with the Protege Management Suite. TCP/IP or Serial (RS-232) ports can be used.

```
SV001 Port
TCP/IP 1
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

TCP/IP Port

The TCP/IP port defines the IP port that is used when communicating between the System Controller and the Protege Management Suite. Ensure that both the controller and the PC software are configured to use the same IP port. This parameter is only used when a TCP/IP port is selected as the Communication Port.

```
SV001 TCP/IP
port: 10000
```

To modify the TCP/IP port (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

RS-232 Speed (Baud Rate)

When an external RS-232 serial port is selected as the communication port this parameter sets the baud rate that is used.

```
SV001 Speed
38400
```

Use the [1] and [3] keys to scroll the available baud rates (150, 300, 1200, 2400, 4800, 9600, 19200, 38400) and press [ENTER] to select the baud rate displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

RS-232 Parity

When an external RS-232 serial port is selected as the communication port this parameter sets the parity that is used.

```
SV001 Parity
No Parity
```

Use the [1] and [3] keys to scroll the available parity and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reporting Options

The Reporting Options contain the advanced features of the Protege SMGT Service. These are used to set up 'offline' reporting of events back to the Protege Management Suite using a TCP/IP connection.

```
SV001 Report Opt
   [-2------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Enable Event Reporting

- Enabled the Service will attempt to send all events back to the Protege System Management Suite both when a connection is established and when it is disconnected. To use this the Server IP and TCP/IP port must also be programmed.
- Disabled events are only uploaded when the Protege Management Suite is connected to the System Controller.

Option 2 – Authentication Required

- Enabled the Service must login to the server before sending events.
- Disabled events are sent with no authentication.

Option 3 – User Login Required

- Enabled the authentication will include the pin number of the user stored at address 0.
- Disabled authentication does not use the pin number.

Option 4 – Prioritize Alarm Events

- Enabled the service will prioritize alarm events to be sent before all other event types.
- Disabled events will be sent to the server in the order they are created.

Option 5 – Enable Poll Events

- Enabled the System Controller will send a poll message to the server at the programmed interval (see Poll Time below).
- Disabled no poll events are created.

Option 6 – Initialize CDMA Modem

- Enabled the Service will send an initialization command when the service starts and then once every 12 hours to make sure the modem is still okay. This is used when an external CDMA modem is used as the connection interface (via an external comm port).
- Disabled no initialization command is sent.

Option 7 – Backup to Secondary IP

- Enabled the service will attempt to send events to the server using the secondary IP address if communication fails on the primary IP address. No poll events are sent to the secondary IP address as poll events are used to prove the primary connection is active.
- Disabled the service will not backup to the secondary IP address on communication failure.

Option 8 – Backup to Monitor Phone

- Enabled the service will attempt to send events to the server using a monitor phone service (the first available service) if communication fails on the primary IP address.
- Disabled the service will not backup to the monitor phone service on communication failure.

Server IP Address

The Server IP Address is the IP address of the Protege System Management Suite that the Controller reports events to when the server is not connected.

```
SV001 Server IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Server Port

The server port configures the service with the remote port number to communicate on.

```
SV001 Server
port: 10002
```

To modify the TCP/IP port (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Backup IP Address

The Backup IP Address is the Backup IP address of the Protege System Management Suite that the Controller reports events to when the server is not connected. Note that this is not a separate server, rather an alternate path for communicating with the server.

```
SV001 Backup IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Backup Port

The backup port configures the service with the remote port number to communicate on.

```
SV001 Server
port: 10002
```

To modify the TCP/IP port (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Transmit Threshold

The transmit threshold configures the service with the number of events that need to be generated before they are transmitted to the Protege Management Suite. Leave this set to 001 to have events sent immediately.

```
SV001 Transmit
threshold: 001
```

To modify the threshold (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Poll Time

The poll time configures the number of seconds between each poll event when the service is configured to send poll events.

```
SV001 Poll
time: 090 secs
```

To modify the poll time (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Encryption

All events sent back to the Protege System Management Suite when the controller is not connected are encrypted. This parameter defines the type of encryption that is used.

```
SV001 Encryption
Default
```

Use the [1] and [3] keys to scroll the available parity and press [ENTER] to select the encryption displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Encryption Key

When AES 128, 192 or 256 bit Encryption is selected this defines the AES key that is used.

```
SV001 Crypt Key
```

To modify or enter a new key use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

Serial Printer Service

To program the serial printer service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen. By default the serial printer service is programmed at SV004 and is running using the programmed TCP/IP address and port 10001.

```
SV001 Ser Type
Serial Printer
```

Use the [1] and [3] keys to scroll the service types until you reach the serial printer selection and press [ENTER] to select the serial printer service type displayed and proceed to the next programmable option for the serial printer service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Number

The communications interface port defines which serial port the controller will use for communication when sending the serial printer output.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the serial printer service will operate. The default value for serial printer is 9600 bits per second. If the speed or configuration is different adjust this setting to suit the host configuration.

```
SV001 Speed
9600
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the serial printer. By default this is set to None however can be adjusted to suit the needs of the host that is connected.

```
SV001 Parity
None
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Area Events Group

The area events group defines which areas events will be sent through the serial printer service. Setting an area group to None (Default) will result in all areas being sent. Setting an area group with a specific group of areas will filter the area related events based on the areas configured in the group.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the available area groups and press [ENTER] to select the area group that is displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

SIA Level 2 Reporting Service

To program the SIA level 2 reporting service ensure that the service that has been selected and is halted. Press the [ENTER] key until the display shows the service type selection screen. The SIA service comprises of 3 levels. The transmission of the information uses a line speed of 300 BAUD and requires a tonal acknowledge.

```
SV001 Ser Type
SIA (Level 2)
```

Use the [1] and [3] keys to scroll the service types until you reach the SIA level 2 reporting selection and press [ENTER] to select the SIA level 2 reporting service type displayed and proceed to the next programmable option for the SIA level 2 reporting service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

SIA Client Code

The SIA client code is used to identify the system to the remote monitoring company when a report is generated. The client code will accept hexadecimal numbers however this will be dependent on the ability of the receiver and should be verified before configuration.

```
SV001 Client
code: 000000
```

Type the appropriate 6 digit client code, after each digit you must press [←] and [→] to move to the next digit. When the desired client code is entered, press [ENTER] to save the programmed setting and move to the next screen. For more information about hexadecimal data entry refer to the section Hexadecimal Data Entry (see page 335).

When using a 4 Digit Account code program the account code in the last 4 locations leaving the first 2 set at 00.

PABX Phone Number

The PABX phone number is dialed to gain an outside line if the system is connected to a internal phone extension. The PABX phone number can also be programmed with a schedule in the case that between certain times the phone line is directly connected with an outside line.

```
SV001 PABX
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Phone Number One

The primary phone number will be dialed by the SIA service when it first is initiated to report an event. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).

```
SV001 Phone 1
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Phone Number Two

The secondary phone number will be dialed by the SIA service if a connection with the central station can not be made on the primary phone number. This may be dialled after the total number of attempts is reached on the primary or until the total number of attempts is reached for the primary and secondary numbers. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).

```
SV001 Phone 2
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. To program a phone number select [MENU, 4, 7, 2]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Backup Phone Number

The backup phone number will be dialed by the SIA service if a connection with the central station can not be made on either of the programmed phone numbers. This will be dialled after the total number of attempts is reached. The backup number will be dialled for the configured number of dialing attempts programmed for the service. For information on the dialing sequence refer to the section Sequential Dialing Attempts (see page 198) and Alternate Dialing Attempts (see page 199).

```
SV001 Backup
None
```

Use the [1] and [3] keys to scroll the available phone numbers and press [ENTER] to select the phone number displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Dial Options

The dial options configure the service as to how it is meant to dial when a reportable event has been generated.

```
SV001 Dial
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 330).

Option 1 - Alternate Dialing Configuration

- Enabled the dialer will use the alternate dialing method. Refer to the Alternate Dialing (see page 199).
- Disabled the dialer will use sequential dialing method. Refer to the Sequential Dialing (see page 198).

Option 2 – Dial Number Using Pulse Dialing

- Enabled the dialer will use pulse dialing to dial out.
- Disabled the dialer will always use DTMF to dial except when Option 3 has been enabled.

Option 3 - Reserved

- Reserved do not modify

Option 4 - Switch To Second Phone Line On Failure

- Enabled the dialer will switch the secondary phone line over and use this to dial if the first phone line fails or fails to communicate.
- Disabled the dialer will use the first phone line.

Option 5 - PABX Phone Number Requires Pause

- Enabled the dialer will insert a pause of 2.5 seconds after the PABX telephone number is dialed.
- Disabled the dialer will dial the PABX and phone number with a standard DTMF inter digit delay.

Option 6, 7 and 8 - Reserved

- Reserved do not modify

Events Options

The events options allow you to filter the type of events that this SIA service will send to the monitoring station.

```
SV001 Events
   [123456--]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Opens

- Enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report opens.

Option 2 - Report Closes

- Enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report closes.

Option 3 - Report Alarms

- Enabled the service will report alarms for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report alarms.

Option 4 - Report Tampers

- Enabled the service will report tampers for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report tampers.

Option 5 - Report Restore

- Enabled the service will report restores for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report restores.

Option 6 - Report Bypass

- Enabled the service will report bypass's for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report bypass's.

Option 7 and 8 - Reserved

- Reserved do not modify

Data Options

The data options are currently reserved and should not be modified from their default settings.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1, 2, 3, 4, 5, 6, 7 and 8 - Reserved

- Reserved do not modify

Miscellaneous Options

The miscellaneous options allow you to program special functions and features for the SIA reporting format.

```
SV001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Modem Service Events

- Enabled the service will provide step by step event information showing the call progression and detailed logging information. This option can be turned on for diagnostic purposes but should not be enabled as large volumes of events will be generated.
- Disabled the dialer will not log call progression events.

Option 2 - 4 Digit Point Reporting Codes

- Enabled the SIA service will use a 4 digit reporting code for the client, the SIA standard supports 6 digits however some receivers do not comply with the full SIA specification or the automation software connected limits the acceptance of large point numbers. Verify the configuration of the receiver with the monitoring company prior to setting these options.

If a 4 Digit Account is to be used program the last 4 digits of the account code with the account ID. For example if you are reporting to account code 9712 program the SIA account code as 009712.

- Disabled the SIA service will send 6 digit point codes.

Option 3 - Pad Area Account Code To 6 Digits

- Enabled the SIA service will pad the upper 2 digits of the 6 digit account code with 00 when sending the client code of an area in place of the service configured account code when multiple account codes are being used. The client code when programmed in an area can only be 4 digits refer to the Area Programming Section (see page 111).

If option 2 is enabled then the SIA service will report all account codes as 4 digits regardless.

- Disabled the SIA service will send 4 digit area account codes.

Option 4 - 5 Digit Zone Code

- Enabled the SIA service will send the zone identifier point using a five digit number. The SIA standard supports 5 digits however some receivers do not comply with the full SIA specification or the automation software connected limits the acceptance of large point numbers. Verify the configuration of the receiver with the monitoring company prior to setting this option.
- Disabled the SIA service will send 4 digit zone identification numbers.

Option 5 - Hexadecimal User Identification Codes

- Enabled the SIA service will send the user identifier using hexadecimal format. When this option is enabled option 6 will not have any affect on the data being sent as hexadecimal codes are always sent using 4 digits only.
- Disabled the SIA service will send decimal zone identification numbers.

Option 6 - 5 Digit User Code

- Enabled the SIA service will send the user identifier point using a five digit number. The SIA standard supports 5 digits however some receivers do not comply with the full SIA specification or the automation software connected limits the acceptance of large point numbers. Verify the configuration of the receiver with the monitoring company prior to setting this option.
- Disabled the SIA service will send 4 digit user identification numbers.

Option 7 and 8 - Reserved

- Reserved do not modify

Area Group

An area group will define which areas this service will process when a reportable event is generated. An area group of None (default) will result in all areas being sent with the service.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Dialing Attempts

The dialing attempts determine how many times the dialer will attempt to dial a number before failure. This setting will be overridden by the modem configuration dependent on the country of installation and local phone authority. For UL and ULC installations this value can not be set above 8. The dialing attempts operate in conjunction with the dialing delay setting.

```
SV001 Dialing
attempts: 008
```

To modify the dialing attempts (000 to 255, a setting of 000 will result in the default of 8 attempts being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Port Open Attempts

The port open attempts determine how many times the service will wait for the modem to become available if another service is already using modem for communication. This operates in conjunction with the port open time settings.

```
SV001 Port open
attempts: 008
```

To modify the port open attempts (000 to 255, a setting of 000 will result in the default of 8 port attempts being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Report Count

The report count if set to a value other than 000 will restrict the service from sending more than the programmed number of reports to the monitoring station. When using multiple reporting paths that potentially can report the same event to 2 or more locations the report count should be programmed with an acceptable limit (Between 8 and 16 is recommended).

```
SV001 Report
count: 000
```

To modify the report count (000 to 255, a setting of 000 will result in an unlimited number of reports being able to be sent), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Handshake Time

The handshake time determines the time it takes for the remote receiving unit to answer and provide a handshake message for the SIA format. By default this is set to 030 seconds and should only be adjusted if a longer than normal call completion is required. When handshakes for lower speed formats are placed in front of the SIA handshake it may be required to increase this time.

```
SV001 Handshake
time: 030
```

To modify the handshake time (000 to 255, a setting below 010 will result in the default of 30 seconds being programmed), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Redial Time

The redial time determines inter phone number dialing timeout. A value of 20 seconds is programmed by default meaning each phone number will be dialled with 20 second intervals from the time the previous call was terminated.

```
SV001 Redial
time: 020
```

To modify the redial time (000 to 255, a setting below 010 will result in the default value of 030 being programmed), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Off Hook PGM

The off hook PGM is activated when the service takes the telephone line and is deactivated when the service completes communication. This PGM setting can be used with remote exchange systems that require ground start communication connections.

```
SV001 Off Hook
pgm: --000:00
```

To modify the off hook PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Report OK PGM

The report ok PGM is activated when the service completes the reporting and the messages have been successfully acknowledge. The PGM is activated when the service returns a reporting complete result OK message. The PGM is not deactivated and should be programmed with a time. Connect to an external audible device to signal that the report was completed. Using this feature with the shorten exit delay for an area allows an end user to verify the communication path on arming of the protected area.

```
SV001 Report Ok
pgm: --000:00
```

To modify the report ok PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

AMX Home Automation Service

To program the AMX home automation service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
AMX
```

Use the [1] and [3] keys to scroll the service types until you reach the AMX home automation selection and press [ENTER] to select the AMX home automation type displayed and proceed to the next programmable option for the AMX home automation service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

DVAC (Surgard) Reporting Service

To program the DVAC (Surgard) reporting service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen. The DVAC (Surgard) service is a hard-line polled communication path utilized in North America across the BELL TELECOM network. A DVAC hardline modem or F1/F2 subset MUST be connected to the communications port using a DVAC modem cable.

```
SV001 Ser Type
DVAC (Surgard)
```

Use the [1] and [3] keys to scroll the service types until you reach the DVAC (Surgard) reporting selection and press [ENTER] to select the DVAC surgard reporting type displayed and proceed to the next programmable option for the DVAC surgard reporting service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The DVAC F1/F2 subset requires a RX/TX and GND connection; this can be connected from the terminal block on the communications interface or the DB9 connector. Refer to the communication PRT-COMM installation manual.

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Number

The communications interface port defines which serial port the controller will use for communication with the DVACS F1 and F2 subset units. Select the communication port that will be plugged in to the unit.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the DVACS service will operate. The default value for DVACS is 150 bits per second. If the speed or configuration is different adjust this setting to suit the host configuration.

```
SV001 Speed
150
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the DVACS F1 and F2 subset units. This will default to Even Parity however this can be adjusted to suit the host configuration.

```
SV001 Parity
Even Parity
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Device Address

When the unit is connected to the DVAC's network it must have a device address programmed. The device address is typically provided by the monitoring station company. The address is programmed in Hexadecimal and can not be above 0xF0 hex.

```
SV001 Device
address: 01
```

Type the appropriate 2 digit device address, after each digit you must press [←] and [→] to move to the next digit. When the desired device address is entered, press [ENTER] to save the programmed setting and move to the next screen. For more information about hexadecimal data entry refer to the section Hexadecimal Data Entry (see page 335).

The device address must be configured for a value below 0xF0, failure to configure the address to an appropriate value will cause the system not to respond.

Events Options

The events options allow you to filter the type of events that this DVAC service will send to the monitoring station.

```
SV001 Events
   [123456--]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Opens

- Enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report opens.

Option 2 - Report Closes

- Enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report closes.

Option 3 - Report Alarms

- Enabled the service will report alarms for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report alarms.

Option 4 - Report Tampers

- Enabled the service will report tampers for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report tampers.

Option 5 - Report Restore

- Enabled the service will report restores for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report restores.

Option 6 - Report Bypass

- Enabled the service will report bypass's for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report bypass's.

Option 7 and 8 - Reserved

- Reserved do not modify

Data Options

The data options are used to log information that is received, make the DVACS service respond to an all call code or respond to odd/even all call requests.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Communication Events

- Enabled the service will log communication events that occur. Please be aware that when used with a polling service such as DVAC's will fill the event buffer with a significant amount of data and should only be used for testing and configuration purposes.

- Disabled the service will not log communication events.

Option 2 - Log DVAC Messages

- Enabled the service will log messages that are sent from the DVAC's network and store these in the event log. Once again this will result in a large number of events being saved.
- Disabled the service will not log DVAC messages.

Option 3 - Respond All Call Command A

- Enabled the service will send an event if it has one ready when the DVAC's host requests an All Call A command.
- Disabled the service will not respond to an All Call Command A.

Option 4 - Respond All Call Command B

- Enabled the service will send an event if it has one ready when the DVAC's host requests an All Call B command.
- Disabled the service will not respond to an All Call Command B.

Option 5 - Respond All Call Odd/Even Address

- Enabled the service will send an event if it has one ready when the DVAC's host requests an All Call A command and the device address is an Odd Address or if the requests an All Call B command and the device address is an Even Address.
- Disabled the service will not respond to an Odd/Even All Call Command.

Option 6, 7 and 8 - Reserved

- Reserved do not modify

When setting the all call options in the data configuration for DVAC only enable one of the available options. Setting more than one of the all call options will result in the first option that is set being used.

Miscellaneous Options

The miscellaneous options are current reserved.

```
SV001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1,2,3,4,5,6,7 and 8 - Reserved

- Reserved do not modify

Area Group

An area group will define which areas this service will process when a reportable event is generated. An area group of None (default) will result in all areas being sent with the service.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reporting Table

With the size of the Protege system the maximum reporting points available in the DVAC service format is easily exceeded, to allow flexibility a reporting table has been created to allow information to be sent using pre-defined zone numbers or values. There are 2 predefined configurations for the reporting tables.

```
SV001 Reporting
table: 000
```

To modify the port open attempts (000 to 255, a setting of 000 will result in the default of 8 port attempts being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Fail To Poll Time

The fail to poll time allows a timer to be triggered on each successful poll from the DVAC's network. This is also used to generate the DVAC service fail to poll trouble zone which can be used to report over a standard phone network using another service. When this timer expires the Fail To Poll PGM output will also be activated.

```
SV001 Poll fail
time: 120 secs
```

To modify the poll fail time (000 to 255, a setting of 000 will result in the default of 120 seconds being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Fail To Poll PGM Output

The fail to poll PGM output is activated when the DVAC service poll fail timer expires and is deactivated when the DVAC service completes a valid communication. This PGM setting can be used to trigger an audible alarm or other indication that DVAC hard line communication has failed.

```
SV001 Poll fail
pgm: --000:00
```

To modify the poll fail PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

ModBUS Slave Service

The ModBUS Slave service has two functions, one of these is to allow remote access to the Protege System Controller from an Industrial Process Control solution or SCADA (System Control and Data Acquisition) System, the other is to allow an Industrial Process, PLC or other device to generate reportable actions within the Protege System Controller (Zone Activation) making reporting of plant and equipment alarms a very simple process.

To program the ModBUS slave service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
ModBUS (Slave)
```

Use the [1] and [3] keys to scroll the service types until you reach the ModBUS slave selection and press [ENTER] to select the ModBUS slave type displayed and proceed to the next programmable option for the ModBUS slave service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The ModBUS Slave Service may require the RS232 serial interface to be converted from a RS485 Signal. Ensure the correct interface is used when interfacing to the Protege System Controller and PRT-COMM. Refer to the communication PRT-COMM installation manual and ACC-485-ISO documentation.

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Number

The communications interface port defines which serial port the controller will use for communication with the ModBUS Master Controller or SCADA application. Select the communication port that will be plugged in to the ModBUS connection.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the ModBUS service will operate. The default value for ModBUS is 9600 bits per second. If the speed or configuration is different adjust this setting to suit the ModBUS master configuration.

```
SV001 Speed
9600
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the ModBUS master. This will default to Even Parity however this can be adjusted to suit the ModBUS master configuration.

```
SV001 Parity
Even Parity
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Device Address

When the unit is connected to a ModBUS communication network it must have a device address programmed. The device address is typically provided by the automation company or defined by the SCADA system that is being connected to. The address is programmed in Hexadecimal and can not be 0x00 or 0xFF.

```
SV001 Device
address: 01
```

Type the appropriate 2 digit device address, after each digit you must press [←] and [→] to move to the next digit. When the desired device address is entered, press [ENTER] to save the programmed setting and move to the next screen. For more information about hexadecimal data entry refer to the section Hexadecimal Data Entry (see page 335).

The device address must be configured for a value below 0xFF and above 0x00, failure to configure the address to an appropriate value will cause the system not to respond. Duplicate address will cause communication failures with the ModBUS Master application.

Data Options

The data configure various communication settings that affect the operation of the ModBUS protocol.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Log Comm Events

- Enabled the service log communication events that occur on the ModBUS system to the event buffer.
- Disabled the communication events will not be logged.

Option 2 – Log Comm Errors

- Enabled the service log ModBUS Communication errors that occur which relate to the requests of certain objects and information outside the bounds of the interface.
- Disabled the errors will not be logged and requests that generate errors will be silently discarded.

Option 3 – Reserved

- Reserved do not modify

Option 4 – Reserved

- Reserved do not modify

Option 5 – Remote Buffer View

- Enabled the service will use the remote buffer for the look up of register values. This is used when the Protege System Controller is used to receive alarms and messages from remote sites that communicate in the Remote ModBUS protocols.
- Disabled the service will use the local objects (Areas, Doors and Zones) to send status and information.

Option 6 – Remote Zone Write

- Enabled the service will allow specific coil address's to interact with the zones on the system. The zones start on the first zone expander. This setting allows remote SCADA applications to activate alarms in the Protege System Controller and report these messages to a standard alarm monitoring station.
- Disabled the coil address's will operate there designated device.

Option 7 and 8 - Reserved

- Reserved do not modify

Fail To Poll Time

The fail to poll time allows a timer to be triggered on each successful poll from the ModBUS Master. When this timer expires the Fail To Poll PGM output will also be activated.

```
SV001 Poll fail
time: 120 secs
```

To modify the poll fail time (000 to 255, a setting of 000 will result in the default of 120 seconds being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Fail To Poll PGM Output

The fail to poll PGM output is activated when the ModBUS service poll fail timer expires and is deactivated when the ModBUS service completes a valid communication. This PGM setting can be used to trigger an audible alarm or other indication that ModBUS communication has failed to operate.

```
SV001 Poll fail
pgm: --000:00
```

To modify the poll fail PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

ModBUS Door Control Group

The door control group will define which doors can be controlled by the ModBUS interface if a door unlock or lock action is requested. The default setting of None allows all doors to be controlled by the interface.

```
SV001 Door Grp
None
```

Use the [1] and [3] keys to scroll the available door groups and press [ENTER] to select the door group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

ModBUS Area Control Group

The area control group will define which areas can be controlled by the ModBUS interface if a area disarm or arm action is requested. The default setting of None allows all areas to be controlled by the interface.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the available area groups and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

ModBUS Remote Reporting Service

To program the ModBUS remote reporting service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
ModBUS (Remote)
```

Use the [1] and [3] keys to scroll the service types until you reach the ModBUS remote reporting selection and press [ENTER] to select the ModBUS remote reporting type displayed and proceed to the next programmable option for the ModBUS remote reporting service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Clipsal C-Bus Automation

To program the Clipsal C-Bus home automation service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

To operate the Clipsal C-Bus service you must connect a serial communications port using the PRT-COMM to a C-Bus PCI (Personal Computer Interface) which allows a high level communication to be transported.

```
SV001 Ser Type
Clipsal C-Bus
```

Use the [1] and [3] keys to scroll the service types until you reach the Clipsal C-Bus home automation selection and press [ENTER] to select the C-Bus home automation type displayed and proceed to the next programmable option for the C-Bus home automation service. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Number

The communications interface port defines which serial port the controller will use for communication with the Clipsal C-Bus PCI Interface. Select the communication port that will be plugged in to the PCI connection.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the Clipsal C-Bus service will operate. The default value for C-Bus is 9600 bits per second. If the speed or configuration is different adjust this setting to suit the C-Bus PCI configuration.

```
SV001 Speed
9600
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the C-Bus PCI. This will default to No Parity however this can be adjusted to suit the C-Bus PCI configuration.

```
SV001 Parity
No Parity
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

TCP/IP Primary IP Address

If the port option 'Ethernet' was selected then you are given the option to enter the IP address of the CNI unit.

```
SV005 Pri IP
191.012.003.077
```

To modify the IP address use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

TCP/IP Primary Port

If the port option 'Ethernet' was selected then you are given the option to enter the TCP/IP Port of the CNI unit.

```
SV005 Primary
port: 09999
```

To modify the port number (00001 to 65534), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Data Options

The data configure various communication settings that affect the operation of the Clipsal C-Bus Interface protocol.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Log Communication Events

- Enabled the service will log communication events that occur on the C-Bus System to the event buffer. It is recommended this is only turned on for commissioning purposes as a large number of events can be generated.
- Disabled the communication events will not be logged.

Option 2 – Log Communication Errors

- Enabled the service will log C-Bus Communication errors that occur which relate to the PCI not being present or not accepting commands.
- Disabled the errors will not be logged and requests that generate errors will be silently discarded.

Option 3,4,5,6,7 and 8 - Reserved

- Reserved do not modify

PCI Fail Time

The PCI fail time allows a timer to be triggered on each successful request from the C-Bus Clipsal PCI Interface. When this timer expires the system will perform a check to see if the PCI is still present and then activate the fail PGM output if a response is not received.

```
SV001 PCI fail
time: 120 secs
```

To modify the fail time (000 to 255, a setting of 000 will result in the default of 120 seconds being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

If the PCI fails to reply to a command or does not send information within the poll fail time the service will go in to a retry mode where it will continually attempt to restart the PCI. This allows recovery of the PCI from a power failure or from being used and reconfigured during a C-Bus Programming session.

PCI Fail PGM Output

The PCI fail output is activated if the PCI is disconnected and the system does not get a valid response to a command. The PGM is deactivated when a valid command is received.

```
SV001 PCI fail
pgm: --000:00
```

To modify the PCI fail PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Intercom High Level Interface

To program the Intercom High Level Interface service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
Intercom
```

Use the [1] and [3] keys to scroll the service types until you reach the Intercom selection and press [ENTER]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Intercom Type

The Intercom Type selects the intercom that will be connected to the Serial Communications Interface.

```
SV001 Intercom
Siedle
```

Use the [1] and [3] keys to scroll the different intercom types and press [ENTER] to select the intercom displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Validation Mode	Function
Siedle	Select when connecting the Siedle range of intercoms. Integrates to the Bus Control module by using an ACC-485 unit and appropriate RS232 cable to the PRT-COMM serial interface.
Sentex Infinity	Select when connecting to the Sentex Infinity Multiple Point intercoms from Chamberlain group. Connects to the serial RS232 output of the intercom, may need a suitable RS485 converter for distances above 15 meters.
Sentex Type L	Select when connecting to the Sentex Type L single channel intercoms from Chamberlain group. Connects to the serial RS232 output of the intercom, may need a suitable RS485 converter for distances above 15 meters.
Enterphone	Select when connecting to the Enterphone intercom system. Connects to the serial RS232 output of the intercom, may need a suitable RS485 converter for distances above 15 meters. The Enterphone unit does not support multi units and therefore does not need to have the intercom address set.

Validation Mode

The Validation Mode determines how the intercom service will grant access and then provide a credit to an elevator car. User Number will validate the user id from the Intercom System with the exact user number in the Protege System Controller, User PIN will validate the user with a PIN number of a user and the User Card will validate the user based on the programmed card number of a user.

```
SV001 Validate
User Number
```

Use the [1] and [3] keys to scroll the different Validation Types and press [ENTER] to select the validation type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Validation Mode	Function
User Number	The user number (index) in to the Protege System controller's user table will be used. This is typically used with fixed user id's for intercom control of doors and floors.
User Number Offset	The user number (index) in to the Protege System controller's user table will be used and an offset can be programmed. This is typically used with fixed user id's for intercom floors.
PIN Number	The PIN number of the programmed user will be used to identify the user from the Intercom System.
Card Number	The Card Number of the programmed user will be used to identify the user from the Intercom System. The family number should be set to 0 unless instructions for the intercom type specify a family number.

Communications Port Number

The communications interface port defines which serial port the controller will use for communication with the intercom that has been configured. Select the communication port that will be plugged in to the intercoms communication interface or RS232 connection.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the Intercom Interface operates. The default value is 9600 bits per second. If the speed or configuration is different adjust this setting to suit the type of intercom that has been selected configuration.

```
SV001 Speed
9600
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the Intercom. This will default to No Parity however this can be adjusted to suit the intercom that has been configured.

```
SV001 Parity
No Parity
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Data Options

The data options configure various communication settings that affect the operation of the Intercom Interface protocol.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Log Communication Events

- Enabled the service will log communication events that occur on the Intercom Communications and store these to the event buffer. It is recommended this is only turned on for commissioning purposes as a large number of events can be generated from the intercom units.
- Disabled the intercom communication events will not be logged.

Option 2 – Log Communication Errors

- Enabled the service will log Intercom Communication errors that occur which relate to the format of the data received, loss of connection (Only specific intercoms) or not being able to decode the information. This should only be turned on for commissioning purposes.
- Disabled the errors will not be logged and requests that generate errors will be silently discarded.

Option 3, 4,5,6,7 and 8 - Reserved

- Reserved do not modify

Intercom 1 Address

The intercom 1 address defines the address received by first intercom slot, up to 4 intercoms can be decoded simultaneously. In some instances certain intercoms are not able to unlock a elevator floor. By configuring the intercom address only the intercoms that are to be used for elevator access are able to be decoded.

```
SV001 Intercom 1
address: 255
```

To modify the intercom address (000 to 255, a setting of 255 will result in this address slot being disabled), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Intercom 2 Address

The intercom 2 address defines the address received by second intercom slot, up to 4 intercoms can be decoded simultaneously. In some instances certain intercoms are not able to unlock a elevator floor. By configuring the intercom address only the intercoms that are to be used for elevator access are able to be decoded.

```
SV001 Intercom 2
address: 255
```

To modify the intercom address (000 to 255, a setting of 255 will result in this address slot being disabled), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Intercom 3 Address

The intercom 3 address defines the address received by third intercom slot, up to 4 intercoms can be decoded simultaneously. In some instances certain intercoms are not able to unlock a elevator floor. By configuring the intercom address only the intercoms that are to be used for elevator access are able to be decoded.

```
SV001 Intercom 3
address: 255
```

To modify the intercom address (000 to 255, a setting of 255 will result in this address slot being disabled), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Intercom 4 Address

The intercom 4 address defines the address received by fourth intercom slot, up to 4 intercoms can be decoded simultaneously. In some instances certain intercoms are not able to unlock a elevator floor. By configuring the intercom address only the intercoms that are to be used for elevator access are able to be decoded.

```
SV001 Intercom 4
address: 255
```

To modify the intercom address (000 to 255, a setting of 255 will result in this address slot being disabled), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Elevator Group

The elevator group that is assigned to this service will be sent the floor group that is programmed in the user access level settings. The elevator group settings in a user are ignored as they may have more elevators available which are not be controlled by the intercom system.

In the case where a bank of 3 elevators are being controlled the elevator group would have the 3 elevators selected in the elevator group. This will result in the floor assigned in the access level of the intercom user being sent to all the elevators in the group.

```
SV001 Elv Group
None
```

Use the [1] and [3] keys to scroll the elevator group setting and press [ENTER] to select the elevator group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Door Group

The door group that is assigned to this service will be unlocked when a valid user is found. This action is independent of the elevator function. The user does not need to have the doors that are assigned in this door group in the door group assigned to their access level. The door group will be unlocked independent of a user setting.

The doors in the door group will be unlocked for the duration of the door lock time setting in each door.

This allows a user to activate the intercom have access granted from the phone system and then the access control system grant access, allowing an event log to be generated of who let someone in to a foyer door, additionally this information can be posted to a DVR or Text Capture software application.

```
SV001 Door Group
None
```

Use the [1] and [3] keys to scroll the door group setting and press [ENTER] to select the door group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Inter Byte Time

The Inter Byte time sets the idle communications time before communications is reset by the Intercom Service. This is used when an intercom does not behave well and sends broken data that has an idle time between bytes. This setting allows a fragmented data packet to still operate correctly. This is typical of some intercoms that send information using proprietary modem and link devices.

```
SV001 Inter Byte
time: 004 secs
```

To modify the inter byte time (000 to 255, a setting of 000 will result in the default of 4 seconds being used), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

User Offset

When the validation of the user number is set to be an offset from the code that is entered the offset quantity needs to be entered in this screen. The offset amount is calculated as the number received from the intercom plus this value (Intercom Packet + Offset Number = User Number).

```
SV001 Offset
value: 00000
```

To modify the offset value (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Intercom Valid Data PGM

The Intercom Valid data output is activated when a packet is decoded correctly. This output will activate regardless of the user being checked and is used to signal a "valid decode" has occurred. The PGM is not deactivated and should have a time set in its PGM programming properties to turn off.

```
SV001 Valid
pgm: --000:00
```

To modify the Valid Data PGM, use the settings as explained in section Entering PGM and PGM Groups *(see page 336)*.

Intercom Access PGM

The Intercom Access output is activated when a packet is decoded correctly and the user is found in the system. The PGM is not deactivated and should have a time set in its PGM programming properties to turn off.

```
SV001 Access
pgm: --000:00
```

To modify the Access PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

GSM Modem Reporting Service

To program the GSM Modem service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
GSM Modem
```

Use the [1] and [3] keys to scroll the service types until you reach the GSM Modem selection and press [ENTER]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The GSM Modem type that is connected must conform to the AT command set defined by the Cellular Modem Standard. We recommend the Wavecom Fast Track modem or similar with a suitable SEPARATE power supply and battery back-up. Do not power the modem unit from the Controller Power Supply.

Communications Port Number

The communications interface port defines which serial port the controller will use for communication with the GSM Modem that has been configured. Select the communication port that will be plugged in to the intercoms communication interface or RS232 connection.

```
SV001 Port
Ext Port 1
```

Use the [1] and [3] keys to scroll the communication ports and press [ENTER] to select the port displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Speed

The communications port speed defines the baud rate at which the GSM Modem operates. The default value is 9600 bits per second and we recommend that this is not changed. If the speed or configuration is different adjust this setting to suit the type of modem that is connected however the majority of modems will default to 9600. If you are not sure about the connection speed verify the modem operation using a terminal program such as (Terraterm or Hyperterminal).

```
SV001 Speed
9600
```

Use the [1] and [3] keys to scroll the communication port speed options and press [ENTER] to select the speed displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Communications Port Parity

The communications port parity defines the parity configuration for the communication with the GSM Modem. This should not be changed from default.

```
SV001 Parity
No Parity
```

Use the [1] and [3] keys to scroll the communication parity options and press [ENTER] to select the parity displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Data Options

The data configure various communication settings that affect the operation of the Intercom Interface protocol.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Log Modem Communication Events

- Enabled the service will log communication events that occur.
- Disabled the communication events will not be logged.

Option 2,3,4,5,6,7 and 8 - Reserved

- Reserved do not modify

Report IP Service

The Report IP Service allows the Protege System controller to send alarm and activation information over an IP connected network. The Report IP Service supports multiple formats and allows the connection to third party reporting if required.

To program the Report IP Service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
Report IP
```

Use the [1] and [3] keys to scroll the service types until you reach the Report IP selection and press [ENTER]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Reporting Protocol

The reporting protocol defines how the IP communication data will be sent to the monitoring station. Various protocols are supported to allow the most comprehensive solution.

```
SV001 Format
Armor IP
```

Use the [1] and [3] keys to scroll the different protocols and press [ENTER] to select the protocol displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Protocol	Function
Armor IP	Armor IP will communicate to the Armor IP server software running on a remotely connected server. The Amour IP Server provides a standard Ademco 685 output and allows routing and redirection of signals to other reception devices such as E-Mail, SMS Messaging and Websites. The Armor IP software is designed to be used with a Concentrator operating in the central station control room.
CID Over IP	CID Over IP communicates a Contact ID message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification. SIA DC09 Specification is currently not released as a formal specification and is subject to change.
SIA Over IP	SIA Over IP communicates a SIA Level 2 message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification. SIA DC09 Specification is currently not released as a formal specification and is subject to change.
AlarmNZ IP	AlarmNZ IP is the IP Communication format used by Alarm New Zealand Limited. By default the AlarmNZ IP service will use the Contact ID reporting format. Information is sent using a login and password and then event information in a ASCII comma separated data format.
Patriot LS30	Patriot LS30 Protocol is the IP Communication format used by Patriot Systems central station automation application. By default the Patriot LS30 service will use a form of Contact ID reporting. Information is sent using a proprietary format and to obtain details the user should contact Patriot Systems directly.

Account Number

The account number for the Report IP Service can be up to 8 digits. An account code with leading zeros will be truncated to send the minimum number of digits, for example the account code 004311 will be sent as 4311. Where there are more digits set in the account code than the format that is selected can send the account number will be truncated.

```
SV001 Account
no: 00000000
```

To modify the account number (setting an account code of 00000000 will disable the service), use the keypad as explained in section Entering Hexadecimal Numbers (see page 335) and press [ENTER]. An area that has an account code set will be used in place of the account code in the service. Verify the account code sending options to see how the account code can be masked with the upper 8 digits (this allows a trouble area to be routed to a service technician automatically).

Primary IP Address

The primary IP address is the IP of the server that has the receiver attached, the receiver can be the Armour IP Server or a IP receiving device.

```
SV001 Pri IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Primary Port

The primary port configures the reporting service with the remote port number to communicate on. Consult the documentation provided with the Receiver software or hardware to find this information. This information may also be different based on how the device is connected to the internet or intranet that you are communicating on.

```
SV001 Primary
port: 09647
```

To modify the port configuration use the keypad as explained in section Entering Decimal Numbers (see page 333) and Press [ENTER] to save the modified data.

Secondary IP Address

The secondary IP address is the IP of the server that has the receiver attached and can be set so that it will be routed through a separate connection. For example a ADSL modem maybe used for primary and a wireless connection for the secondary communications. For higher security it may also be desirable to have two service providers of internet.

```
SV001 Sec IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Secondary Port

The Secondary port configures the reporting service with the remote port number to communicate on for the secondary IP. By using this information in connection with the secondary IP a specific route can be set for this connection.

```
SV001 Primary
port: 09647
```

To modify the port configuration use the keypad as explained in section Entering Decimal Numbers (see page 333) and Press [ENTER] to save the modified data.

Back Up Service

A back up service can be programmed to allow the IP reporting functions to be backed up by a telephone dialer or similar. Using a back up service can be beneficial to allow link failures and internet access to be reported over an alternate connection.

```
SV001 Back Up
None
```

Use the [1] and [3] keys to scroll the service selection and press [ENTER] to select the service to be used for back up. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Back up Service Time

If both IP connections fail, the Report IP service will switch to a back up service operating over another media. The time before this occurs can be set using the 'Backup time' setting.

```
SV005 Backup
time: 00030 secs
```

To modify the time until backup (00001 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Server Polling Time

The polling time is set to schedule periodic connections with the server. The polling messages sent to the receiver will depend on the format. Some formats require that the polling time be set at both the controller and receivers, in this case ensure that this setting matches the setting provided by the central monitoring station company.

```
SV001 Polling
time: 120 secs
```

Edit the polling time to a value of 10 to 255 seconds, any number below 10 will disable the polling being sent to the server. Use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

The polling time set will periodically send the polling message for the AlarmNZ IP and Patriot LS30 reporting formats a standard contact ID message with the code 602 will be sent for area 00 and point 999. In some cases these are used only to reset a polling time and not generated as alarms in the Central Station.

Events Options

The events options allow you to filter the type of events that this Report IP service will send to the monitoring station.

```
SV001 Events
   [123456--]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Report Opens

- Enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report opens.

Option 2 - Report Closes

- Enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report closes.

Option 3 - Report Alarms

- Enabled the service will report alarms for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report alarms.

Option 4 - Report Tampers

- Enabled the service will report tampers for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report tampers.

Option 5 - Report Restore

- Enabled the service will report restores for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report restores.

Option 6 - Report Bypass

- Enabled the service will report bypasss for the zones that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Disabled the dialer will not report bypass's.

Option 7 and 8 - Reserved

- Reserved do not modify

Data Options

The data options are used to log information that is received, make the DVACS service respond to an all call code or respond to odd/even all call requests.

```
SV001 Data
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Log Acknowledge Events

- Enabled the service will log acknowledge communication events.
- Disabled the service will not log acknowledge communication events.

Option 2 - Log Poll Accept Events

- Enabled the service will log and event when the polling has been accepted by the remote host receiver.
- Disabled the service will not log polling messages.

Option 3 – Log Communications Retry

- Enabled the service will log a communications retry that occurs because of a network failure or loss of service.
- Disabled the service will not log communications retries.

Option 4 – Log Communications Failure

- Enabled the service will log an event when communications have failed completely and the service is waiting on another attempt.
- Disabled the service will not log the communications failure.

Option 5, 6, 7 and 8 - Reserved

- Reserved do not modify

When setting the log polling events and log acknowledgments the event buffer can be filled very quickly. Use these options to check the connectivity of the service and then turn them off after commissioning has been completed.

Area Group

An area group will define which areas this service will process when a reportable event is generated. An area group of None (default) will result in all areas being sent with the service.

```
SV001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area group selection and press [ENTER] to select the area group displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Link Me (IO)

The Link Me (IO) Service provides an interface for Protege System Controllers to communicate together through the linking of PGM outputs. This service maps PGMs on one System Controller to a second System Controller so they follow the state of the primary System Controller.

To program the Link Me Service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
Link Me (IO)
```

Use the [1] and [3] keys to scroll the service types until you reach the Link Me selection and press [ENTER]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Primary IP Address

The primary IP address is the IP of the Protege System Controller that is being linked with.

```
SV001 Pri IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Primary Port

The primary port configures the TCP/IP port the two System Controllers will communicate over.

```
SV001 Primary
port: 09647
```

To modify the port configuration use the keypad as explained in section Entering Decimal Numbers (see page 333) and Press [ENTER] to save the modified data.

Polling Time

The polling time is set to schedule periodic connections with the other system controller.

```
SV001 Poll
time: 120 secs
```

Edit the polling time to a value of 10 to 255 seconds, any number below 10 will disable the polling being sent to the controller. Use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Function

The function defines how the service will operate; it can either send or receive data. When set to Send Data the controller will inform the second controller of the PGMs being controller. When set to Receive Data the controller will listen to the secondary controller and update it's PGM status according to the received values.

```
SV001 Function
Send Data
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

PGM Mapping Start

The PGM mapping start defines the first PGM that is mapped between the 2 controllers.

```
SV001 Start
pgm: CP001:01
```

To modify the PGM, use the settings as explained in section Entering PGM and PGM Groups.

PGM Mapping Count

The PGM Mapping count defines the number of PGM's that are mapped between the 2 controllers. This count can extend past modules, refer to the PGM addressing to work out the addressing of PGMs.

```
SV001 PGM Link
count: 008
```

Edit the polling time to a value of 10 to 255 seconds, any number below 10 will disable the polling being sent to the controller. Use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Poll OK PGM

The Poll OK PGM defines the PGM that is activated when communication is established between the 2 controllers.

```
SV001 Poll OK
pgm: CP001:02
```

To modify the PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Poll Fail PGM

The Poll Fail PGM defines the PGM that is activated when communication fails between the 2 controllers.

```
SV001 Poll Fail
pgm: CP001:02
```

To modify the PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

General Options

The general options define how the service operates.

```
SV001 General
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options *(see page 336)*.

Option 1 - 8 - Reserved

- Reserved do not modify

VizIP DVR IP Alarm Integration

The VizIP DVR IP Alarm Integration Service provides an interface for Protege System Controllers to communicate to a DVR over IP that has the VizIP IP communication protocol. This service maps PGMs on the System Controller to the alarm outputs from the DVR, eliminating the need to have physical wiring connections from the DVR to the Protege System Controller.

To program the VizIP Service ensure that the service that has been selected is halted. Press the [ENTER] key until the display shows the service type selection screen.

```
SV001 Ser Type
VizIP DVR
```

Use the [1] and [3] keys to scroll the service types until you reach the Viz IP selection and press [ENTER]. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to "Start With The Operating System" (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

BACnet Service

The BACnet service allows external devices to monitor and control the state of PGMs on the Protege system. For further information on the BACnet service please refer to *Application Note AN_087 BACnet IP Integration*.

Service Mode

The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to *Start With The Operating System* (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts. Manual control of the service can be set by using the Manual option for the service mode.

```
SV001 Ser Mode
Start with O/S
```

Use the [1] and [3] keys to scroll the available operating modes and press [ENTER] to select the operating mode displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Primary IP Address

The primary IP address is the IP of the device to which the BACnet service will communicate.

```
SV001 Pri IP
000.000.000.000
```

To modify the IP address use the keypad as explained in section Entering Decimal Numbers (see page 333). Press [ENTER] to save the Octet that is being entered and move to the next Octet or the next screen once all four have been completed.

Primary Port

The primary port configures the TCP/IP port through which the BACnet communications will operate.

```
SV001 Primary
port: 47808
```

To modify the port configuration use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER] to save the modified data.

Device ID

Enter the Device ID for the BACnet service.

```
SV005 Device
04444
```

To modify the device ID use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER] to save the modified data.

Start PGM

This is the first PGM in a range of PGMs to which the BACnet binary values are mapped.

```
SV005 Start PGM
no: 00000
```

To modify the start PGM number use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER] to save the modified data.

Total Number of PGMs

Enter the total number of PGMs (in a contiguous range) that will be mapped to BACnet binary values.

```
SV005 total PGM
no: 00008
```

To modify the total number of PGS setting use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER] to save the modified data.

Telephone Numbers

To access the telephone number programming menu login using a valid installer code and then select [MENU, 4, 7, 2]. The screen displays "Phone No to modify" as shown in the following example.

```
Phone No to
modify: PN001
```

Phone numbers are defined so that a telephone number and if required a secondary number depending on a schedule can be assigned to a service that communicates using a modem or telephone connection.

Selecting a Telephone Number to Modify

Each telephone number is assigned a unique telephone number from 001 to 016. Your system will be limited to specific number of telephone numbers that are defined in the selected profile. For information on profiles refer to the Advanced Programming Section (see page 201).

```
Phone No to
modify: PN001
```

Type the appropriate 3-digit service number or use the [🡻] and [🡹] keys to scroll the available services. When the desired service appears on the screen, press [ENTER] to program and control the selected service.

Telephone Number Name

If the selected telephone number has a name associated (some telephone numbers do not have a name associated with them) the name programming screen will be shown.

```
PN001 Name
*Phone No 001
```

To scroll telephone numbers by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected telephone number use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the telephone name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Operating Schedule

The operating schedule for the telephone number determines when the telephone number is valid to be dialed and if it will use a secondary telephone if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operating of functions based on a 7 day week and 24 hour clock. For more information on the programming of the schedule refer to the Schedule Programming section (see page 272).

The telephone number schedule allows you for example to report messages during a normal day (8am to 5pm) to one telephone number or monitoring station and then outside of these hours reporting them to another location.

```
PN001 Schedule
None
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Secondary Telephone Number

A secondary telephone number when programmed will be used when the schedule of the telephone number that is being programmed is not valid. The schedule of the secondary telephone number must be valid or set to none.

```
PN001 Secondary
None
```

Use the [1] and [3] keys to scroll the secondary telephone number selection and press [ENTER] to select the telephone number displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). Programming a secondary telephone number that uses the current telephone number being edited will perform no function.

Telephone Number

Program the telephone number that you want to assign to this telephone number entry.

```
PN001 Number
```

Use the numeric keys [0] to [9] to enter the telephone number. When the number has been programmed press the [ENTER] key. To clear the telephone number displayed press the [DISARM] key.

When using a telephone number that requires a number to be dialled before gaining an outside line program the individual number or series of numbers in to a telephone number and call this 'PABX Access'. When programming the service or function that requires the telephone number you will also be able to select a telephone number for PABX access.

Sequential Dialing Attempts

Sequential dialing is used by default and results in the reporting phone numbers programmed in the service being dialed sequentially. In the following example, a service is programmed with a two telephone numbers (Phone 1 and Phone 2) and a backup telephone number. The number of dialing attempts is set to 8 and the Use Alternate Dialing Method option is disabled.

Success After 5th Dialing Attempt With Phone Number 1

In the following example, the Controller was able to communicate with the central station with the programmed phone number 1 on the 5th attempt.

Dial Attempt Number	Phone Number Dialed	Result
1	Phone Number 1	Fail
2	Phone Number 1	Fail
3	Phone Number 1	Fail
4	Phone Number 1	Fail
5	Phone Number 1	Success (Report OK)

Success After 1st Dialing Attempt With Back Up Phone

In the following example, the Controller was able to communicate with the central station only after the backup phone number was used. This resulted in the opening of the reporting failure trouble zone as a result of the reporting failure. This is subsequently sealed on the next valid report from the backup phone number.

Dial Attempt Number	Phone Number Dialed	Result
1	Phone Number 1	Fail
2	Phone Number 1	Fail
3	Phone Number 1	Fail
4	Phone Number 1	Fail
5	Phone Number 1	Fail
6	Phone Number 1	Fail
7	Phone Number 1	Fail
8	Phone Number 1	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)
1	Back Up Phone Number	Success (Report OK) Trouble Zone CP001:06 Closed)

Failure After All Dialing Attempts

In the following example, the Controller fails to communicate using any of the programmed phone and backup phone numbers.

Dial Attempt Number	Phone Number Dialed	Result
1	Phone Number 1	Fail
2	Phone Number 1	Fail
3	Phone Number 1	Fail
4	Phone Number 1	Fail

Dial Attempt Number	Phone Number Dialed	Result
5	Phone Number 1	Fail
6	Phone Number 1	Fail
7	Phone Number 1	Fail
8	Phone Number 1	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)
1	Back Up Phone Number	Fail
2	Back Up Phone Number	Fail
3	Back Up Phone Number	Fail
4	Back Up Phone Number	Fail
5	Back Up Phone Number	Fail
6	Back Up Phone Number	Fail
7	Back Up Phone Number	Fail
8	Back Up Phone Number	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)
1	Phone Number 2	Fail
2	Phone Number 2	Fail
3	Phone Number 2	Fail
4	Phone Number 2	Fail
5	Phone Number 2	Fail
6	Phone Number 2	Fail
7	Phone Number 2	Fail
8	Phone Number 2	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)

Alternate Dialing Attempts

Alternate dialing is an option available in the majority of the reporting services and results in the reporting phone numbers programmed in the service being dialed in an alternative sequence. In the following example, a service is programmed with two telephone numbers (Phone 1 and Phone 2) and a backup telephone number. The number of dialing attempts is set to 8 and the Use Alternate Dialing Method option has been enabled.

If alternate dialing is enabled for the reporting service it is recommended that the monitoring company is informed and that they can make the appropriate programming arrangements.

Success After 5th Dialing Attempt With Phone Number 1

In the following example, the Controller was able to communicate with the central station with the programmed phone number 1 on the 5th attempt. As can be seen the back up phone number is dialed on each alternative failure. This is an extreme example most reports would have been received on the backup phone typically on the second attempt.

Dial Attempt Number	Phone Number Dialed	Result
1	Phone Number 1	Fail
1	Back Up Phone Number	Fail

Dial Attempt Number	Phone Number Dialed	Result
2	Phone Number 1	Fail
2	Back Up Phone Number	Fail
3	Phone Number 1	Fail
3	Back Up Phone Number	Fail
4	Phone Number 1	Fail
4	Back Up Phone Number	Fail
5	Phone Number 1	Success (Report OK)

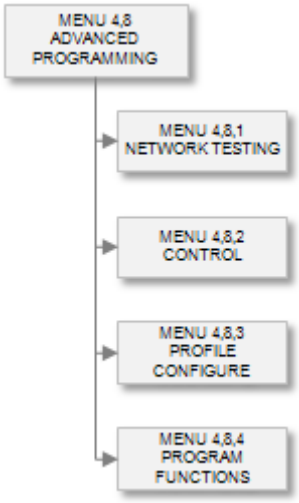
Success After 2nd Dialing Attempt With Phone Number 2

In the following example, the Controller was able to communicate with the central station only after phone number 2 was dialed for the second time. This resulted in the opening of the reporting failure trouble zone as a result of the reporting failure. This is subsequently sealed on the next valid report.

Dial Attempt Number	Phone Number Dialed	Result
1	Phone Number 1	Fail
1	Back Up Phone Number	Fail
2	Phone Number 1	Fail
2	Back Up Phone Number	Fail
3	Phone Number 1	Fail
3	Back Up Phone Number	Fail
4	Phone Number 1	Fail
4	Back Up Phone Number	Fail
5	Phone Number 1	Fail
5	Back Up Phone Number	Fail
6	Phone Number 1	Fail
6	Back Up Phone Number	Fail
7	Phone Number 1	Fail
7	Back Up Phone Number	Fail
8	Phone Number 1	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)
8	Back Up Phone Number	Fail (Trouble Zone CP001:06 Opened, Failure To Communicate)
1	Phone Number 2	Fail
2	Phone Number 2	Fail (Trouble Zone CP001:06 Closed)

Advanced

The advanced menu contains special functions, tests and allows control of objects in the Protege system. The control of every PGM, Door and Zone is possible to allow for immediate diagnostic and testing to be completed.



Network functions including, updating, reset, offline, online and network protect are performed in the advanced section.

To go to the advanced menu select [MENU, 4, 8]. You can then select from the menu items presented or scroll the menu using the [🡅] and [🡇] keys.

Network Offline Module View

Viewing modules that are offline is performed by using the offline module view function in the advanced network section. To enter the offline view select [MENU, 4, 8, 1, 1] the follow display explains the screen information.

- Select the offline network menu item. The display will show that the system is scanning all modules to see if any have gone offline.

  ```
  Checking offline
  modules....
  ```

- If the system finds that a module is offline the module type and serial number will be displayed and a prompt asking the user to check for the next offline module.

  ```
  RD061 S:AC92B39D
  Next module ?
  ```

  The screen shows that PRT-RDI2 located at address 061 is registered in the system with serial number AC92B39D has gone offline or failed to contact the controller. Press the [🡇] key to check the next module.

If the module was removed from the system or changed to another address use the network update function to update all of the modules.

- When the scanning for offline modules is completed or there are no more modules to scan the display will show the message below.

  ```
  Offline list
  Completed.
  ```

To scan again press the [🡇] or press the [MENU] key to return to the main menu.

Network Online Module View

Viewing modules that are online is performed by using the online module view function in the advanced network section. To enter the module online view function select [MENU, 4, 8, 1, 2] the follow display explains the screen information.

- Select the offline network menu item. The display will show that the system is scanning all modules to see if any have gone offline.

  ```
  Checking online
  modules....
  ```

- If the system finds that a module is offline the module type and serial number will be displayed and a prompt asking the user to check for the next offline module.

  ```
  KP001 S:9781711F
  Next module ?
  ```

  The screen shows that PRT-KLCD located at address 001 is registered in the system with serial number 9781711F is online and operating correctly. Press the [🡻] key to check the next module.

- When the scanning for online modules is completed or there are no more modules to scan the display will show the message below.

  ```
  Online list
  Completed.
  ```

To scan again press the [🡻] or press the [MENU] key to return to the main menu.

Network Module Reload

Reloading modules on the network will program the module with the configuration settings that are programmed in the controller. This should be performed when programming of the system is completed. To enter the module update function select [MENU, 4, 8, 1, 3] the following display explains the screen information and actions that are performed.

- Select the update option from the network menu. The display will prompt to ask if you are sure you want to reload the modules. If you want to continue with the update press the [ENTER] key, to cancel press the [MENU] key.

  ```
  Reload modules
  are you sure?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the module update has proceeded.

  ```
  Reload modules
  started....
  ```

  If the screen displays a message that the update process could not start this is because another network function has taken priority. When this is completed try to perform the update again.

Each module will be programmed with the configuration information.

Network Init and Reboot

Init and reboot modules on the network will program the module with the configuration settings that are programmed in the controller and then perform a reset of the module. This should be performed when programming of the system is completed. To enter the module update function select [MENU, 4, 8, 1, 4] the following display explains the screen information and actions that are performed.

- Select the update init item from the module menu. The display will prompt to ask if you are sure you want to update and init the modules. If you want to continue with the update press the [ENTER] key, to cancel press the [MENU] key.

  ```
  Init and reboot
  are you sure?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the module update has proceeded.

```
Init and reboot
started....
```

If the screen displays a message that the update process could not start this is because another network function has taken priority. When this is completed try to perform the update again.

Each module will be programmed with the configuration information and then reset so that the information is loaded in to the module. The keypad that is currently being used will eventually be reset and the display will inform the user that this is taking place.

Module Network Statistics

The module network logs an abundant number of statistics that can be used for fault diagnostics and network performance analysis. The information below may be requested by support staff to help diagnose potential problems. To select the network statistics menu select [MENU, 4, 8, 1, 5] the following display explains the screen information and actions that are performed.

- When the menu item is selected the first statistics will be displayed. To move to the next display press [🡻], to cancel press the [MENU] key. The first screen will show the network receive and transmit octet count.

  ```
  *Net Stats*
  R:34620  T:78265
  ```

  R = Received number of octets (8 Bit communication bytes)

  T = Transmitted number of octets (8 Bit communication bytes)

- Pressing the [🡻] key will display the next statistics screen showing the overrun and break error counts.

  ```
  *Net Stats*
  O:00000  B:00003
  ```

  O = Overrun errors occur when the system is heavily loaded and are a normal part of operation. However the number of overrun errors should not be large in comparison to receive and transmit numbers.

  B = Break detect errors occur when the system detects that a device has held the line in a locked state for longer than the allowable time. This is also part of normal operation.

- Pressing the [🡻] key will display the next statistics screen showing the parity and framing error counts.

  ```
  *Net Stats*
  Z:00000  F:00027
  ```

  Z = Parity errors should not normally occur during normal operation however they may occur and do not affect the system.

  F = Framing errors will occur during normal operation and do not affect the performance of the system or how the system operates.

- Pressing the [🡻] key will display the next statistics screen showing the process related communication get and post functions. These relate to internal tasks that pass the information on the module network to other parts of the Protege Operating System.

  ```
  *Net Stats*
  G:00000  P:00003
  ```

  G = Get errors occur when the system is heavily loaded and the available free memory for the communication receive function becomes exhausted. This can occur normally but should not have high values in most cases this should always be 0.

  P = Post errors occur when the system is heavily loaded and the available free memory for the communication send function becomes exhausted. This can occur normally but should not have high values in most cases this should always be 0.

- Pressing the [🡻] key will display the next statistics screen showing the checksum and general UART (Universal Asynchronous Receiver and Transmitter) errors.

  ```
  *Net Stats*
  C:00000  U:00021
  ```

  C = Checksum errors occur when a packet sent does not contain a valid checksum. This can occur frequently depending on the environment and network loading.

  U = UART errors occur in normal operation and are the accumulated value of all the individual UART errors.

- Pressing the [🡻] key will display the next statistics screen showing the acknowledge failure and lost packet errors.

  ```
  *Net Stats*
  A:00002  L:00003
  ```

  A = Acknowledge errors occur when the module that a communication command was sent to did not acknowledge. These errors occur in normally operating systems.

  L = Lost packet errors occur when the system loses a packet it tries to send to a module because the module is not connected or the communication to the module has been lost.

Offline User Update

An offline user update will update all offline users and programming to intelligent modules. This should be performed when programming of the system is completed and all intelligent modules are online. To enter the offline user update function select [MENU, 4, 8, 1, 6] the following display explains the screen information and actions that are performed.

- Select the offline update option from the network menu. The display will prompt to ask if you are sure you want to upload offline users to the modules. If you want to continue with the offline update press the [ENTER] key, to cancel press the [MENU] key.

  ```
  Offline update
  are you sure?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the offline update has proceeded.

  ```
  Offline update
  started....
  ```

  If the screen displays a message that the offline update process could not start this is because another network function has taken priority. When this is completed try to perform the update again.

Each intelligent reader expander module will be programmed with the user and configuration information.

Network Security

Securing the network will prevent any module from being added to the network and should be done once all testing is completed and the system is operational. To enter the network secure function select [MENU, 4, 8, 1, 7] the following display explains the screen information and actions that are performed. By default a network is not secured to allow modules to be added to the system.

- Select the secure network menu item. The display will prompt to ask if you are sure you want to secure the network. If you want to continue with the network secure press the [ENTER] key, to cancel press the [MENU] key.

  ```
  Secure Net
  are you sure?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the network secure was successful.

  ```
  Secure Net
  started...
  ```

  If the screen displays a message that the network secure process could not be completed this may be due to a network update process being operational.

  Any security violations or errors will result in the Module Security Trouble zone activating on the controller.

- If the network security is already enabled and maintenance is required on the system the network security must be disabled. The display will prompt to ask if you are sure you want to disable the network security. If you want to continue with the network security disable command press the [ENTER] key, to cancel press the [MENU] key.

  ```
  Un-Secure Net
  are you sure?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the network security disable request was successful.

```
Un-Secure Net
started...
```

If the screen displays a message that the network security process could not be disabled this will be due to a network update process being operational. What for the update process to complete and then request the network security disable again.

Cancel Module Update

In some cases it may be required to cancel an update of the modules. This can be done using the cancel module update option. The cancel module update will prompt the user for the update type to cancel if it is running an update or inform the user that there is nothing to cancel. To cancel a module update function select [MENU, 4, 8, 1, 8] the following display explains the screen information and actions that are performed.

- Select the cancel update option from the network menu. The display will present a message with the current update in process. If you want to continue and cancel the update process shown press the [ENTER] key, to exit press the [MENU] key or any other key.

  ```
  Offline update
  cancel?
  ```

- Pressing the [ENTER] key the keypad will display the message below if the offline update has been canceled.

  ```
  Offline update
  canceled....
  ```

The screen will then return to the menu item that was selected.

Reset Network Statistics

To reset the network statistics press the [FORCE] key while in any of the statistic display screens. The statistic counters will not increment past 65535.

Testing Functions

The testing menu only contains one entry, the view menu. This allows you to view the status of zones and trouble zones, control PGM's and control doors. To enter the testing menu select [MENU, 4, 8, 2] you can then scroll the menu for the available options.

Viewing Zones

To access the zone view menu login using a valid installer code and then select [MENU, 4, 8, 2, 1, 1]. The screen displays "Select zone to view" as shown in the following example.

```
Select zone to
view: CP001:01
```

Type the appropriate module type, module address and zone number or use the [↓] and [↑] keys to scroll the available zones. When the desired zone number appears on the screen, press [ENTER] to view the selected zone number.

When selecting a Zone the zone address is entered using the Module Type, Module Address and the number of the zone, this is called Protege Object Notation.

Information on the Protege Object Notation and how it applies to programmable objects within the Protege System refer to the Object Notation Section (see page 330).

Zone Status Display

When the zone is selected the name of the zone will be displayed on the top line and the state of the zone will be shown on the bottom line.

```
Warehouse PIR
is TAMPERED
```

Use the [🡻] and [🡹] keys to scroll the available zones while in the view screen or press the [🡸] to return to the zone selection. Pressing the [ARM] key will toggle the display between the name and the zone identification. Each zone is assigned a unique identification that uses the Protege Notation.

```
CP001:01 Zone
is TAMPERED
```

The display will show the zone state and will depend on the resistor configuration option programmed for the zone that is being viewed. The possible states that can be displayed are:

OPEN	Zone is opened.
CLOSED	Zone is closed.
SHORT	Zone is shorted out or a wiring fault has occurred.
TAMPERED	Zone wiring is cut or faulty.

By default the zone name will be shown on the top line of the screen however if no name is programmed or the name is blank it may be desirable to view the device and address of the module that the zone is connected to. To view the input in the system it is connected on press the [ARM] key, the [ARM] key can be pressed repeatedly to toggle between the two display options.

Viewing Trouble Zones

To access the trouble zone view menu login using a valid installer code and then select [MENU, 4, 8, 2, 1, 2]. The screen displays "Trouble zone to view" as shown in the following example.

```
Trouble zone to
view: CP001:01
```

Type the appropriate module type, module address and trouble zone number or use the [🡻] and [🡹] keys to scroll the available trouble zones. When the desired trouble zone number appears on the screen, press [ENTER] to view the selected trouble zone number.

When selecting a trouble zone the trouble zone address is entered using the Module Type, Module Address and the number of the zone, this is called Protege Object Notation.

Information on the Protege Object Notation and how it applies to programmable objects within the Protege System refer to the Object Notation Section (see page 330).

Trouble Zone Status Display

When the trouble zone is selected the name of the trouble zone will be displayed on the top line and the state of the trouble zone will be shown on the bottom line. The Trouble Zone names are not able to be modified and assigned by default.

```
CP001 Tamper
is OPEN
```

Use the [🡻] and [🡹] keys to scroll the available trouble zones while in the view screen or press the [🡸] to return to the trouble zone selection. Pressing the [ARM] key will toggle the display between the name and the trouble zone identification. Each zone is assigned a unique identification that uses the Protege Notation.

The display will show the trouble zone states as detailed below.

OPEN	Zone is opened.
CLOSED	Zone is closed.

Controlling PGM Outputs

To access the PGM output viewing and control menu login using a valid installer code and then select [MENU, 4, 8, 2, 1, 3]. The screen displays "Select PGM to view" as shown in the following example.

```
Select PGM to
view: CP001:01
```

Type the appropriate module type, module address and PGM number or use the [🡻] and [🡹] keys to scroll the available PGM's. When the desired PGM number appears on the screen, press [ENTER] to view and control the selected PGM number.

When selecting a PGM the address is entered using the Module Type, Module Address and the number of the PGM on the module, this is called Protege Object Notation.

Information on the Protege Object Notation and how it applies to programmable objects within the Protege System refer to the Object Notation Section (see page 330).

PGM Output Status Display

When the PGM is selected the name of the PGM will be displayed on the top line and the state of the PGM will be shown on the bottom line.

```
Bell 1 Siren
is OFF
```

Use the [🡻] and [🡹] keys to scroll the available PGM's. Pressing the [ARM] key will toggle the display between the name and the PGM identification. Each PGM Output is assigned a unique identification that uses the Protege Notation.

```
CP001:01 PGM
is OFF
```

In the view screen, press the [1] key to activate the PGM for the programmed value, press the [2] key to deactivate a PGM that is activated and press the [3] key to activate the PGM latched. Press the [🡸] to return to the PGM selection display.

The display will show the PGM states listed below.

OFF	PGM is deactivated.
ON	PGM is activated.
ON (Timed)	PGM is activated for a time period.

By default the PGM name will be shown on the top line of the screen however if no name is programmed or the name is blank it may be desirable to view the device and address of the module that the PGM is connected to. To view the PGM output in the system it is connected on press the [ARM] key, the [ARM] key can be pressed repeatedly to toggle between the two display options.

Viewing Door Status

To access the door status and control menu login using a valid installer code and then select [MENU, 4, 8, 2, 1, 4]. The screen displays "Select Door to view" as shown in the following example.

```
Select Door to
view: DR001
```

Type the appropriate door number or use the [🡻] and [🡹] keys to scroll the available doors. When the desired door number appears on the screen, press [ENTER] to view and control the selected door number.

Door Control and Status Display

Each door will display the status of the door inputs that are controlling the door and the state of the lock output that is controlled by the door configuration.

```
*Door 001
(Closed)(Locked)
```

Use the [🡻] and [🡹] keys to scroll the available doors while in the view screen, press the [1] key to unlock the door for the programmed unlock time, press the [2] key to lock the door, press the [3] key to activate the door latched, press the [4] key to change the door lockdown state and press the [5] key to cancel the door lockdown. Press the [🡸] to return to the Door selection display.

The display will show the door input states listed below.

CLOSED	Door is closed
OPEN	Door is open
FORCED	Door is forced open
PREALM	Door is in a pre-alarm open condition
LEFTOP	Door has been left open

The display will show the door lock states listed below.

LOCKED	Lock PGM is deactivated
ACCESS	Lock PGM is activated by a user entry
SCHED	Lock PGM is activated by schedule
TIMED	Lock PGM is activated for time period by manual control
LATCH	Lock PGM is activated latched by manual control
ENTRY	Lock PGM is activated request to enter
EXIT	Lock PGM is activated request to exit
MENU	Lock PGM is activated keypad control
AREA	Lock PGM is activated by area
FIRE	Lock PGM is activated by fire control programmable function
LD-ALL	Door is in Lockdown and will only unlock for a super user
LD-ENT	Door is in Lockdown with Entry Allowed
LD-EXT	Door is in Lockdown with Exit Allowed
LD-E+E	Door is in Lockdown with Entry and Exit Allowed

Profile Configuration

Profiles configure the local onboard and expanded memory (if it is present) with the number of supported records (Users, Events, Doors ...). To enter the profile menu select [MENU, 4, 8, 3] you can then scroll the menu for the available options.

Changing Profiles

To change profiles login using a valid installer code and then select [MENU, 4, 8, 3, 1]. The screen displays "Select profile" as shown in the following example.

```
Select profile
Standard
```

Eight profiles are provided that allow the configuration of numerous record structures and setups, it is also possible to customize the number of records that the controller will function with by selecting the custom profile.

Use the [1] and [3] keys to scroll the available profiles. When the desired profile is displayed on the screen, press [ENTER] to load the selected profile. For more information about the list control data entry refer to the section List Control Data Entry (see page 335). To view a profiles size and structures select [MENU, 4, 8, 3, 2].

When selecting a Profile a warning screen will be displayed informing the user that the option will reset the panel and that they need to upload the information to be able to preserve the information from one profile to the next.

When the [ENTER] key is pressed a warning is immediately displayed to the user with a rejection tone beep, to cancel press the [MENU] key or the [CLEAR] key to log out.

```
This will reset
all panel data !

Upload the panel
to backup data.

Press [ENTER] to
continue.

Press [MENU] or
[CLEAR] to exit.
```

To continue with the default you must press the **[ENTER]** key, this will reset the panel and setup the internal memory structures to the selected profile.

Programmable Function Configuration

Programmable functions are used to perform special processing of actions when a particular event or operation occurs. For example resetting users anti-passback status to the unknown state or controlling a group of doors.

To enter the programmable function menu login using a valid installer code and then select [MENU, 4, 8, 4]. The screen displays "Function to modify" as shown in the following example.

```
Function to
modify: FN001
```

Functions are a vital component to the Protege System and allow many variations of logic, process and automation to be performed. Functions are small independent functions within the Protege that are used to process information or perform specialized control functions.

When the functions appears on the screen, press [ENTER] to program the function. The maximum number of functions that can be programmed is limited by your system's memory and configured profile.

Functions that attempt to perform circular referenced input and output (that is the use of a PGM output to change the state of the same PGM output) will automatically be halted and a programming error event will be generated.

Selecting a Function to Modify

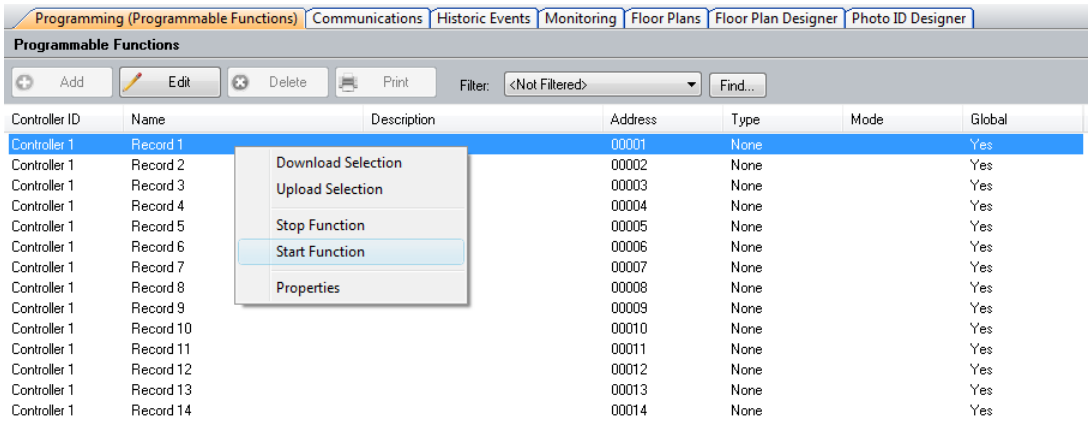
Each function is assigned a unique function number from 001 to 250. Your system will be limited to specific number of functions that are defined in the selected profile. For information on profiles refer to the section Advanced Programming Section (see page 201).

```
Function to
modify: FN001
```

Type the appropriate 3-digit function number or use the [🡻] and [🡹] keys to scroll the available functions. When the desired function appears on the screen, press [ENTER] to program and control the selected function.

Controlling Functions (Starting and Stopping)

For a function to start performing the actions that it is programmed for you must start the function. This is achieved by selecting the Start or Stop function by right-clicking the particular function.



Functions cannot be programmed if they are running and a message warning the user that the function can be viewed only. To edit the function you must stop the function and then proceed with programming.

If the function is running and changes are made to the function the system will not save these to the programmed function.

Type Of Function

The type of function that is programmed will determine the operation that this function will perform. This will also determine the programming screens that follow in each of the sub sections as the programming of functions can contain many features and options dependent on this selection.

```
FN001 Func Type
None
```

Use the [1] and [3] keys to scroll the function types and press [ENTER] to select the function type displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

The following table includes a complete explanation of each function type that is programmable in the Protege System.

Function Type	Description
None	The function will perform no actions and controls no resources. This function can not be started or halted.
Logic Control	Performs logic operations on Programmable Outputs. Can be used to AND, OR, XOR, FOLLOW, NOT FOLLOW the programmable outputs and activate a programmable output as a result of function. When using logic control that will follow a status the system will activate the associated output as a result of the logic function however if the output is changed from the state it will be updated 30 seconds later, this prevents endless loops from occurring while still ensuring an output will result in it being maintained.
Area Control	Can be used to arm or disarm an area based on the status of a PGM output. This can only check the area status in follow mode every 60 seconds.
RTHP Control	Use to manage a Roof Top Heat Pack air conditioning system and can operate up to 4 stages of heat and cool as well as two stages of dehumidification.
Floor Temping	Use to manage a floor tempering system with single stage heat and cool. Duct and floor sensors inputs as well as reverse and forward operational modes.

Function Type	Description
Value Compare	A direct comparison between two data registers with programmable hysteresis and activate time as well has a high and low PGM output. Ideal for the control of lighting circuits based on daylight sensor inputs
Ripple PGM	Ripples on and ripples off up to 8 PGM outputs from an enable PGM. Ideal for staging on large current devices and multiple lighting circuits.
Door Control	Can be used to lock and unlock a door or door group based on the status of a input.

The functions require specific programming for the type that is selected, the following details the programming information for each function type.

- Logic Control (see page 211)
- Area Control (see page 214)
- RTHP Controller (see page 217)
- Value Compare (see page 230)
- Ripple PGM Output (see page 232)
- Door Control (see page 235)
- Floor Temping Control (see page 225)

Logic Control Function

To program the logic control function ensure that the function you have selected is halted. Select the function type selection screen as shown below for logic control.

```
FN001 Func Type
Logic Control
```

Use the [1] and [3] keys to scroll the function types until you reach the logic control selection and press [ENTER] to select the logic control function type displayed and proceed to the next programmable option for the logic control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will mean the function will only run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the logic control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Logic Action

The logic action determines what logical operation or action is performed on the Inputs that are programmed in the following screens. There are eleven different options for the logical control function.

```
FN001 Action
None
```

Use the [1] and [3] keys to scroll the logic action types until you reach the required action that you want to be performed and then press [ENTER] to proceed to the next programmable option for the logic control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

- Follow and **Test**

  The output follows the programmed input one state and will retest the input state continually.

Input One	Output
ON	ON
OFF	OFF

  Test Action - If the output state is changed externally or is part of another programmable function the programmable function will only restore the output state after 30 seconds has elapsed. This time is only used if the programmable function was NOT responsible for the change in state.

- **Not Follow and Test**

  Performs the same function as above however the output is inverted (NOT). This logic action is a test action, consult the follow and test action for an explanation of the Test Function.

Input One	Output
ON	OFF
OFF	ON

- **Pulse On**

  The pulse on action will turn the output ON only when the input one has transitioned from an off to an on state. The output will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output
	ON

- **Not Pulse On**

  The not pulse on action will turn the output OFF only when the input one has transitioned from an off to an on state. The output will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	OFF

- **Pulse Off**

  The pulse on action will turn the output ON only when the input one has transitioned from an ON to an OFF state. The output will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output
	ON

- **Not Pulse Off**

  The not pulse off action will turn the output OFF only when the input one has transitioned from an ON to an OFF state. The output will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	OFF

- **OR Follow and Test**

The OR follow and test action will perform a logical OR operation on Input One and Input Two with the output changing according to the logic operation.

The logic output will use the test function to restore the output to the logic state if it is changed by an external operation.

Input One	Input Two	Output
OFF	OFF	OFF
ON	OFF	ON
OFF	ON	ON
ON	ON	ON

- AND Follow and Test

The AND follow and test action will perform a logical AND operation on Input One and Input Two with the output changing according to the logic operation.

Input One	Input Two	Output
OFF	OFF	OFF
ON	OFF	OFF
OFF	ON	OFF
ON	ON	ON

- NOR Follow and Test

The NOR follow and test action will perform a logical NOR operation on Input One and Input Two with the output changing according to the logic operation. A NOR operation works the same as an OR operation however the output is a NOT of the logic operation.

The logic output will use the test function to restore the output to the logic state if it is changed by an external operation.

Input One	Input Two	Output
OFF	OFF	ON
ON	OFF	OFF
OFF	ON	OFF
ON	ON	OFF

- NAND Follow and Test

The AND follow and test action will perform a logical NAND operation on Input One and Input Two with the output changing according to the logic operation. A NAND operation works the same as an AND operation however the output is a NOT of the logic operation.

Input One	Input Two	Output
OFF	OFF	ON
ON	OFF	ON
OFF	ON	ON
ON	ON	OFF

- XOR Follow and Test

The XOR follow and test action will perform a logical Exclusive OR operation on Input One and Input Two with the output changing according to the logic operation.

Input One	Input Two	Output
OFF	OFF	OFF
ON	OFF	ON

OFF	ON	ON
ON	ON	OFF

Input One PGM / Memory Register

Input one selects the input source to the logic process that is being configured. All logic control functions use at least one input source. Input one must be programmed with a valid input source, if an input source is selected that is not valid when the function is started an error will be generated and the function suspended. An input source can be a PGM (Programmable Output) or a Memory Register.

```
FN001 Input one
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Input Two PGM / Memory Register

Input two selects the input source to the logic process that is being configured when two inputs are used to obtain a output. An input source can be a PGM (Programmable Output) or a Memory Register.

```
FN001 Input two
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Output PGM / Memory Register

Output PGM selects the PGM output to activate or deactivate as a result of the action being performed by the logic process.

```
FN001 Output
pgm: --000:00
```

To modify the output PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Area Control Function

To program the area control function ensure that the function you have selected is halted. Select the function type selection screen as shown below for Area Control.

```
FN001 Func Type
Area Control
```

Use the [1] and [3] keys to scroll the function types until you reach the area control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the area control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the area control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Area Action

The action determines what action is performed on the area or area group that is programmed as a result of the Input PGM. For key switch arming or simple arming of an area from a zone input use the area control options in the zone type configuration. Refer to the Zone Type Programming (see page 99).

```
FN001 Action
None
```

Use the [1] and [3] keys to scroll the action types until you reach the required action that you want to be performed and then press [ENTER] to proceed to the next programmable option for the area control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

- Follow and Test

  The area status follows the programmed input one state and will retest the input state continually.

Input One	Area Control
ON	ARM
OFF	DISARM

  Test Action - If the output state is changed externally or is part of another programmable function the programmable function will only restore the output state after 30 seconds has elapsed. This time is only used if the programmable function was NOT responsible for the change in state.

- Not Follow and Test

  Performs the same function as above however the area control function is inverted (NOT). This logic action is a test action, consult the follow and test action for an explanation of the Test Function.

Input One	Area Control
ON	DISARM
OFF	ARM

- Pulse On

  The pulse on action will arm the area only when the input one has transitioned from an off to an on state. The area will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Area Control
	ARM

- Not Pulse On

  The not pulse on action will disarm the area only when the input one has transitioned from an off to an on state. The area will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Area Control
	DISARM

- Pulse Off

  The pulse on action will arm the area only when the input one has transitioned from an ON to an OFF state. The area will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Area Control
	ARM

- Not Pulse Off

  The not pulse off action will disarm the area only when the input one has transitioned from an ON to an OFF state. The area will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Area Control
	DISARM

Input One PGM

Input one selects the input source to the area control process that is being configured. All area control functions use at least one input source. Input one must be programmed with a valid input source, if an input source is selected that is not valid when the function is started an error will be generated and the function suspended. An input source can be a PGM (Programmable Output) or a Memory Register (Special area of memory that can be used store values and monitor internal system functions).

```
FN001 Input one
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Control Area

The control area selects the area to control as a result of the action being performed by the programmable function. To control an area group leave the control area option set to none and proceed to the Control Area Group. Selecting both an area and an area group will result in only the area being controlled and the area group being ignored. Programming an area and an area group will result in the area group not being used.

```
FN001 Area
None
```

Use the [1] and [3] keys to scroll the action types until you reach the required action that you want to be performed and then press [ENTER] to proceed to the next programmable option for the area control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Control Area Group

The control area group selects the area group to control as a result of the action being performed by the programmable function. To control an area leave the control area group section set to none and program an area in the control area section. Programming an area and an area group will result in the area group not being used.

```
FN001 Area Grp
None
```

Use the [1] and [3] keys to scroll the area groups until you reach the required group and then press [ENTER] to proceed to the next programmable option for the area control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

RTHP Control Function

The RTHP (Roof Top Heat Pump / Roof Top Heat Pack) programmable function allows the direct control of multiple stage Roof Top Heat Pumps used for large retail or commercial space temperature control. There is a substantial number of configuration screens for the RTHP unit and a working knowledge of Air Conditioning and Temperature Set Point configuration is essential in setting up the correct operation of the programmable function.

```
FN001 Func Type
RTHP Control
```

Use the [1] and [3] keys to scroll the function types until you reach the RTHP control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the RTHP control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator. Setting the run once option for the RTHP will result in NO operation being performed and the function stopping a short time after it is started.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the RTHP control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Enabled Control PGM

Enabled Control PGM is set when the RTHP is to run and will operate only when the enabled PGM is on. If no enabled PGM is set the RTHP will run continuously. This allows the RTHP to operate only during the times that the space is occupied. The signal can also be a memory register or a Boolean (bit) value from the selected memory register.

```
FN001 Enabled
pgm: --000:00
```

To modify the occupy PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Fault PGM

The fault control PGM is set when a fault condition has occurred and the RTHP is to shutdown. This allows the RTHP to shutdown in the shortest possible time without causing any damage to the system. In the case of a fire shutdown the system must have a fire PGM programmed.

```
FN001 Fault
pgm: --000:00
```

To modify the fault PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336). To select a data register press the stay key, the following screen will be shown and a memory register location can be selected. To view the memory register locations refer to appendix memory registers.

Fire PGM

The fire control PGM is monitored NOT controlled by the function and when the fire PGM has been activated, typically by an external fire alarm input, the RTHP will gracefully shut down the air conditioning system and halt operation until the fire alarm has been cleared. This PGM could be the PGM used to deactivate smoke dampers and other related equipment in the HVAC control system.

```
FN001 Fire
pgm: --000:00
```

To modify the fire PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336). Do not set a PGM group for the fire or other monitored PGM's as this will have no action in the control system and will be the same as not setting a PGM value.

Fan Control PGM

The fan PGM is activated when the RTHP starts to operate and is started 30 seconds prior to any heating, cooling or dehumidification is required allowing it to ramp up to the desired speed.

```
FN001 Fan
pgm: --000:00
```

To modify the fan PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Cooling Stage 1 PGM

The cool 1 PGM is activated when the RTHP has a requirement for cooling and the cooling stage demand value has been exceeded for the first stage. The cooling 1 PGM will typically be used to control the first stage of the cooling system.

```
FN001 Cool 1
pgm: --000:00
```

To modify the cool 1 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Cooling Stage 2 PGM

The cool 2 PGM is activated when the RTHP has a requirement for cooling and the cooling stage demand value has been exceeded for the second stage. The cooling 2 PGM will typically be used to control the second stage of the cooling system.

```
FN001 Cool 2
pgm: --000:00
```

To modify the cool 2 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Cooling Stage 3 PGM

The cool 1 PGM is activated when the RTHP has a requirement for cooling and the cooling stage demand value has been exceeded for the third stage. The cooling 3 PGM will typically be used to control the third stage of the cooling system.

```
FN001 Cool 3
pgm: --000:00
```

To modify the cool 3 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Cooling Stage 4 PGM

The cool 1 PGM is activated when the RTHP has a requirement for cooling and the cooling stage demand value has been exceeded for the fourth stage. The cooling 4 PGM will typically be used to control the fourth stage of the cooling system.

```
FN001 Cool 4
pgm: --000:00
```

To modify the cool 1 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Heating Stage 1 PGM

The heat 1 PGM is activated when the RTHP has a requirement for heating and the heating stage demand value has been exceeded for the first stage. The heating 1 PGM will typically be used to control the first stage of the heating system.

```
FN001 Heat 1
pgm: --000:00
```

To modify the heat 1 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Heating Stage 2 PGM

The heat 2 PGM is activated when the RTHP has a requirement for heating and the heating stage demand value has been exceeded for the second stage. The heating 2 PGM will typically be used to control the second stage of the heating system.

```
FN001 Heat 2
pgm: --000:00
```

To modify the heat 2 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Heating Stage 3 PGM

The heat 3 PGM is activated when the RTHP has a requirement for heating and the heating stage demand value has been exceeded for the third stage. The heating 3 PGM will typically be used to control the third stage of the heating system.

```
FN001 Heat 3
pgm: --000:00
```

To modify the heat 3 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Heating Stage 4 PGM

The heat 4 PGM is activated when the RTHP has a requirement for heating and the heating stage demand value has been exceeded for the fourth stage. The heating 4 PGM will typically be used to control the fourth stage of the heating system.

```
FN001 Heat 4
pgm: --000:00
```

To modify the heat 4 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Dehumidification Stage 1 PGM

The dehumidification stage 1 PGM is activated when the RTHP has a requirement for dehumidification. The dehumidification process will typically open the first stage of the hot gas reheat valves located in the RTHP unit.

```
FN001 Dehumid 1
pgm: --000:00
```

To modify the dehumidification stage 1 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Dehumidification Stage 2 PGM

The dehumidification stage 2 PGM is activated when the RTHP has a requirement for dehumidification and the humidity is above the hysteresis value plus the setpoint. The dehumidification process will typically open the second stage of hot gas reheat valves located in the RTHP unit.

```
FN001 Dehumid 2
pgm: --000:00
```

To modify the dehumidification stage 2 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Base Data Register

The Base data register is used as the first register in the list of registers used to configure, program and control the RTHP. The only registers that are not included in the base registers are ones that must link to an analog input or analog output for external sensors (Temp, Humidity or Dampers). A base data register setting MUST be set.

```
FN001 Base data
reg: 00000
```

To modify the base data register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Base Data Register Offset

Register Offset	Register Function
0	*Heating Set Point* The heating set point determines the temperature that the RTHP will heat the space to and is compared with the temperature sensor connected to the Space Temp input.
1	*Cooling Set Point* The cooling set point determines the temperature that the RTHP will cool the space to and is compared with the temperature sensor connected to the Space Temp input.
2	*Relative Humidity Set Point* The relative humidity set point determines at what humidity level the RTHP will go in to a dehumidification cycle and drive the plant to reduce this amount. The relative humidity set point when exceeded is added or subtracted using the Hysteresis value to prevent oscillation of the humidity modes.
3	*Heating Hysteresis Setting* The heating hysteresis value is added to the heating set point to allow the plant to drive slightly beyond the set point. This allows specific heating and cooling tuning. Setting a value of 0 is not recommended as it can cause the system to oscillate between the dead band the heating modes.

Register Offset	Register Function
4	*Cooling Hysteresis Setting* The cooling hysteresis value is subtracted from the cooling set point to allow the plant to drive slightly below the set point. This allows specific heating and cooling tuning. Setting a value of 0 is not recommended as it can cause oscillations between the dead band and cooling modes.
5	*Relative Humidity Hysteresis Setting* The relative humidity hysteresis value is subtracted or added depending if the set point has already been exceeded to the relative humidity set point. This allows the relative humidity cycles to be tuned. Setting a value of 0 is not recommended as it can cause the system to oscillate between the relative humidity states.
6	*Warm Up Set Point* If the warm up set point is not equal to 0 the system will check the space temperature against the warm up set point when the occupied relay is activated. If the internal temp is below the warm up set point the system will close the fresh air damper and drive the heating to achieve the heating set point. Once set point is reached the unit will operate in a normal mode.
7	*Fresh Air Cooling Set Point* If the fresh air cooling set point is not 0 the system will check the fresh air temperature when a cooling demand exists and modulate the dampers to allow free cooling. The system will remain in the free cooling mode for the time set by the free cooling time.
8	*Stage 1 Demand Value* The stage one demand value is the amount of plant error that is required to activate the first stage of cooling or heating. Plant error is calculated using a custom PI loop. The error is accumulated using the settings for the Integral Value and Hysteresis Settings. The error value is the difference between the set point and the current space temperature with the addition of the accumulated error.
9	*Stage 2 Demand Value* The stage two demand value is the amount of plant error that is required to activate the second stage of cooling or heating.
10	*Stage 3 Demand Value* The stage three demand value is the amount of plant error that is required to activate the third stage of cooling or heating.
11	*Stage 4 Demand Value* The stage four demand value is the amount of plant error that is required to activate the fourth stage of cooling or heating.
12	*Current RTHP Mode* The current mode that the RTHP is operating in. The RTHP modes are listed in the section below.
13	*Current Plant Error* The current plant error is the error in the temperature value difference between the set point and the current temperature. This value is for display only and used to calculate the drive required for the RTHP to obtain the desired set point.
14	*Integral Error* The integral error is the amount of raw calculated error using the integral portion of the PI loop used for the control of the RTHP unit and is calculated ONLY in a cooling or heating requirement mode.

Register Offset	Register Function
15	*Integral Term* The integral term is the result of a calculation using the integral gain and the integral error to obtain a value that can be used to add with the Plant Error to ensure that the heating and cooling set points are meet with the maximum amount of efficiency.
16	*Output Error* The output error is the absolute output error at the current point and can be used as a guide when tuning the RTHP. The output error represents the Integral Term added with the raw Plant Error values. The output error is used to calculate the staging of the heating and cooling within the RTHP unit.
17	*Integral Gain* The integral gain is the gain of the integral portion of the PI loop and is a division of the actual integral error amount that is used to form the calculation. The integral gain will divide by 1, 2, 4, 8 etc by setting a value of 1,2,3,4 ... 15. **If a value of 0 is programmed for the integral gain the system will not use integral within the PI loop and it will be disabled.**
18	*Integral Maximum Value* As the integral value is a calculated value that is continually updated it can easily reach a saturation point where the plant can not meet the integral and plant error values. In this case we program a limit that will stop the integral from increasing beyond a recoverable point.
19	*Integral Calculation Time* The integral calculation time is a time base used by the integral portion of the PI loop to update the Integral Error. It is advised not to set this below a value of 30 seconds.
20	*Fresh Air Damper Normal Setting* The fresh air damper normal setting is the value that is output on the fresh air economies analog output used to control the fresh air damper position. This value allows the system to be tuned to an appropriate setting to allow the require Litres Per Second of fresh air to enter the RTHP.

Roof Top Heat Pack Mode Definition

Register Offset	Register Function
0	*RTHP Idle Condition* The programmable function is idle and no processing is taking place.
1	*RTHP Waiting For Start Signal* The programmable function is waiting for the enable PGM signal to be controlled to an ON state to start operation. This is usually managed by a schedule or the alarm status. When the signal is received the Fan PGM will be activated and the programmable function will enter a delay of 30 seconds before starting.
2	*RTHP Warm Up Check* If the RTHP is programmed to enter a warm up state at the start of operation the temperature will be checked here to verify if the warm up temperature is above the current space temperature if it is then the RTHP will enter the warm up mode.
3	*RTHP Warm Up Space* When in warm up mode the RTHP is driven to full capacity to get the space above the heating set point in the fastest possible time. Once the temperature reaches this level the system will operate normally.

Register Offset	Register Function
4	*RTHP Deadband Process* The deadband process is where the RTHP will wait for a condition that is outside the set points for heating, cooling or dehumidification.
5	*On Call For Space Heating* The space temperature is below the heating set point and the function to start the heating process is active. This will activate the stages required to bring the temperature up to the heating set point.
6	*On Call For Space Cooling* The space temperature is above the cooling set point and the function to start the cooling process is active. This will activate the stages required to bring the temperature down to the cooling set point.
7	*On Call For Fresh Air Space Cooling* The space temperature is above the cooling set point and the outside air is below the free air cooling set point, the RTHP will oscillate the fresh air economizer in attempt to cool the space using the fresh air intake. This will remain active until the temperature is below the cooling set point or if the free cooling fails to achieve set point in the set time (Free Cooling Time) mode 6 will be entered.
8	*Heating Stage Off* Heating stages are being turned off progressively due to the set point being reached.
9	*Cooling Stage Off* Cooling stages are being turned off progressively due to the set point being reached.
10	*Dehumidification Cooling Plus Reheat* Dehumidification is required and the current set point is above the cooling set point. The dehumidification stage will be entered in an attempt to get the humidity under control.
11	*Dehumidification Transition* The dehumidification process is in a transition between the dehumidification requirements and cooling.
12	*Dehumidification Heating* Dehumidification is required and the current set point is below the heating set point. The dehumidification stage will be entered in an attempt to get the humidity under control while an attempt is also made to obtain heating set point.
13	*Dehumidification Heating Stage Off* Dehumidification and heating stages are deactivated because the humidity has come under control or the cooling set point (other side of the dead band setting) has been reached.
14	*Dehumidification Cooling Stage Off* Dehumidification and cooling stages are deactivated because the humidity has come under control or the heating set point (other side of the dead band setting) has been reached.
15	*Dehumidification Stage Off* Dehumidification stages are deactivated because the humidity has reached set point and dehumidification is no longer required.
16	*RTHP Shutting Down* The RTHP is completing an orderly shutdown of the currently activated stages and the fan control signals.

Register Offset	Register Function
17	*Fault Condition* A fault condition has activated that has caused the RTHP to shut down. This condition is typical of a smoke damper closing or other mechanical input that will result in the RTHP shutting down.
18	*Fire Condition* A fire alarm condition has been activated that has caused the RTHP to shut down.

Space Temperature Register

The space temperature register is the register that is updated by an analogue module input channel connected to a temperature sensor. The space temperature is typically from a sensor located within the space the RTHP is controlling.

```
FN001 Space temp
reg: 00000
```

To modify the space temperature register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

If you are unsure how the RTHP operates and what action is going to be started as a result in the change in the input registers you can specify the register to be a normal register outside the analogue module range. This will allow an installer to modify the values with the Protege System Management Suite and visually see the mode change in the RTHP without the need to physically connect the RTHP.

Space Humidity Register

The space humidity register is the register that is updated by an analogue module input channel connected to a humidity sensor. The space humidity sensor is typically located within the space the RTHP is controlling at a height of 1.5 to 2.5 meters above floor level.

```
FN001 Space rh
reg: 00000
```

To modify the space humidity register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

External Fresh Air Temperature Register

The external fresh air temperature register is the register that is updated by an analogue module input channel connected to a temperature sensor. The external fresh air temperature is typically from a sensor located within fresh air intake of the RTHP in the cowling section. The fresh air temperature sensor is used to calculate the ability to cool the space with direct fresh air and is calculated prior to a demand for cooling.

```
FN001 Fresh temp
reg: 00000
```

To modify the fresh temperature register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Economiser Damper Register

The Base data register is used as the first register in the list of registers used to configure, program and control the RTHP. The only registers that are not included in the base registers are ones that must link to an analog input or analog output for external sensors (Temp, Humidity or Dampers). A base data register setting MUST be set.

```
FN001 Space rh
reg: 00000
```

To modify the base data register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Floor Tempering Control Function

The Floor Tempering programmable function allows the direct control of a single stage floor tempering system that controls a duct mounted heater and/or cooling compressor. The support for one heating and one cooling state is provided as well as a forward and reverse operation.

```
FN001 Func Type
Floor Temping
```

Use the [1] and [3] keys to scroll the function types until you reach the Floor Temping selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the Floor Temping control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator. Setting the run once option for the RTHP will result in NO operation being performed and the function stopping a short time after it is started.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the floor temping function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Enabled Control PGM

Enabled Control PGM is set when the Floor Temping is to run and will operate only when the enabled PGM is on. If no enabled PGM is set the Floor Temping will run continuously. Programming a PGM that is activated by a schedule allows the floor temping to operate only during the times that the space is occupied.

```
FN001 Enabled
pgm: --000:00
```

To modify the enable PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Fault PGM

The fault control PGM is set when a fault condition has occurred and the Floor Temping is to shutdown. This allows the Floor Temping to shutdown in the shortest possible time without causing any damage to the system. In the case of a fire shutdown the system must have a fire PGM programmed.

```
FN001 Fault
pgm: --000:00
```

To modify the fault PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Fire PGM

The fire control PGM is monitored NOT controlled by the function and when the fire PGM has been activated, typically by an external fire alarm input, the floor tempering will gracefully shut down the system and halt operation until the fire alarm has been cleared. This PGM could be the PGM used to deactivate smoke dampers and other related equipment in the HVAC control system.

```
FN001 Fire
pgm: --000:00
```

To modify the fire PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336). Do not set a PGM group for the fire or other monitored PGM's as this will have no action in the control system and will be the same as not setting a PGM value.

Fan Control PGM

The fan PGM is activated when the floor tempering starts to operate and is started 30 seconds prior to any heating or cooling. The direction of the fan (forward and reverse) is determined by the forward and reverse PGM outputs. If a fan on signal is not required use the forward and reverse PGM outputs to drive the appropriate contactors.

```
FN001 Fan
pgm: --000:00
```

To modify the fan PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Forward PGM

The forward PGM is used to drive the fan in the forward direction this will circulate air from the intake through the heating element and towards the floor. In the forward mode the temperature at the floor is below the set point.

```
FN001 Forward
pgm: --000:00
```

To modify the forward PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Reverse PGM

The reverse PGM is used to drive the fan in the reverse direction this will circulate air from the floor and return this to the intake. In the reverse mode the temperature at the floor is above the set point.

```
FN001 Reverse
pgm: --000:00
```

To modify the reverse PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Manual Forward PGM

The manual forward PGM is monitored by the floor temping function and if it is activated the function will operate in forward mode regardless of the floor temperature setting.

```
FN001 Man Fwd
pgm: --000:00
```

To modify the Manual Forward PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Manual Reverse PGM

The manual reverse PGM is monitored by the floor temping function and if it is activated the function will operate in reverse mode regardless of the floor temperature setting. If the manual forward and reverse PGM's are activated the floor tempering system will operate in the forward mode and ignore the reverse PGM setting.

```
FN001 Man Rev
pgm: --000:00
```

To modify the Manual Reverse PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Cool On PGM

The cool on PGM is activated when the floor tempering has a requirement for cooling if the floor tempering system does not have a cooling compressor do not set the cool on PGM.

```
FN001 Cool on
pgm: --000:00
```

To modify the cool on PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Heat On PGM

The heat on PGM is activated when the floor tempering has a requirement for heating and is activated only in the forward direction.

```
FN001 Heat on
pgm: --000:00
```

To modify the heat on PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Base Data Register

The Base data register is used as the first register in the list of registers used to configure, program and control the Floor Tempering system. The only registers that are not included in the base registers are ones that must link to an analog input or analog output for external sensors (Temp, Humidity or Dampers). A base data register setting MUST be set.

```
FN001 Base data
reg: 00000
```

To modify the base data register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Base Data Register Offset

Register Offset	Register Function
0	*Tempering Set Point* The tempering set point determines the temperature that the floor tempering will operate at. This value is compared with the floor temperature input to determine if cooling or heating is required and the direction of the fan.
1	*Floor Temperature Hysterisis Setting* The floor temperature hysterisis value is subtracted from the floor temperature set point to allow the floor tempering to drive slightly above and below the set point.
2	*Duct Temperature Set Point* This sets the maximum value for the duct sensor and is used to control the heating of the duct air.
3	*Duct Temperature Hysterisis Setting* The duct temperature heating hysterisis value is added to the duct heating set point to allow the floor tempering to drive slightly beyond the set point. This setting prevents the floor tempering system from oscillating between the dead band and heating modes.
4	*Current Floor Tempering Mode* The current mode that the floor tempering is operating in. The floor tempering modes are listed in the section below.

Floor Tempering Mode Definition

Register Offset	Register Function
0	*Floor Tempering Idle Condition* The programmable function is idle and no processing is taking place.
1	*Floor Tempering Waiting For Start Signal* The programmable function is waiting for the enable PGM signal to be controlled to an ON state to start operation. This is usually managed by a schedule or the alarm status. When the signal is received the Fan PGM will be activated and the programmable function will enter a delay of 30 seconds before starting.
2	*Floor Tempering Waiting Check* If the floor tempering is checking if it requires to operate in a manual or automatic mode.
3	*Floor Tempering Dead Band Process* The dead band process is where the floor tempering will wait for a condition that is outside the set point for tempering of the floor or heating the duct.
4	*Floor Heating* The floor temperature is below the floor heating set point and the function to start the heating process is active. This will activate the floor heater that is required to bring the temperature up to the heating set point.
5	*Floor Cooling* The floor temperature is above the floor heating set point and the function to start the cooling process is active. This will operate the floor tempering in reverse and disable the duct heater.
6	*Manual Heating Forward* The manual forward (heating) override PGM is active and the floor tempering is operating in Manual Heating mode.

Register Offset	Register Function
7	*Manual Cooling Reverse* The manual reverse (cooling) override PGM is active and the floor tempering is operating in Manual Cooling mode.
8	*RTHP Shutting Down* The floor tempering is completing an orderly shutdown of the currently activated outputs and the fan control signal.
9	*Fault Condition* A fault condition has activated that has caused the floor tempering to shut down. This condition is typical of a smoke damper closing or other mechanical input that will result in the floor tempering shutting down.
10	*Fire Condition* A fire alarm condition has been activated that has caused the floor tempering to shut down.
11	*Mode Delay* The mode has changed during a controlled operation either from Manual to Auto or Auto to Manual and the function has entered a delay period.

Floor Temperature Register

The floor temperature register is the register that is updated by an analogue module input channel connected to a temperature sensor located at the floor level which is operated by the floor tempering system. The floor temperature is typically received from a sensor located within the floor area being controlled.

```
FN001 Floor temp
reg: 00000
```

To modify the floor temperature register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

If you are unsure how the Floor Tempering function operates and what action is going to be started as a result in the change in the input registers you can specify the register to be a normal register outside the analogue module range. This will allow an installer to modify the values with the Protege System Management Suite and visually see the mode change in the Floor Tempering without the need to physically connect the Floor Tempering to mechanical devices.

Duct Temperature Register

The duct air temperature register is the register that is updated by an analogue module input channel connected to a temperature sensor. The duct air temperature is typically from a sensor located within the duct downstream (when operating in forward mode) of the duct fan.

```
FN001 Duct temp
reg: 00000
```

To modify the duct temperature register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Value Compare Function

The compare value function allows the comparison of an input value with predefined values in data registers. This allows the activation of a low and high PGM output when the comparison is over the set point and the hysterisis time.

```
FN001 Func Type
Value Compare
```

Use the [1] and [3] keys to scroll the function types until you reach the Value Compare selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the Value Compare function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator. Setting the run once option for the value compare function will result in NO operation being performed and the function stopping a short time after it is started.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the value compare function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Enabled Control PGM

Enabled Control PGM is set when the value compare function is to run and will operate only when the enabled PGM is on. If no enabled PGM is set the value compare function will run continuously. This allows the value compare function to operate only during the times that the resulting PGM is required.

```
FN001 Enabled
pgm: --000:00
```

To modify the enabled PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

High PGM

The High PGM output will activate when the input data register (usually an input from an analog register) is above the set point plus the hysterisis value and has been for the duration of the hysterisis time. The high PGM will turn off if the input value is below the set point value.

```
FN001 High
pgm: --000:00
```

To modify the High PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Low PGM

The Low PGM output will activate when the input data register (usually an input from an analog register) is below the set point minus the hysterisis value and has been for the duration of the hysterisis time. The low PGM will turn off if the input value is above the set point value.

```
FN001 Low
pgm: --000:00
```

To modify the low PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Base Data Register

The Base data register is used as the first register in the list of registers used to configure, program and control the Value Compare. The only registers that are not included in the base registers are ones that must link to an analog input or analog output for external sensors (Temp, Daylight (LUX), Water Level). A base data register setting MUST be set to ensure the system can pick up the set points and data values.

```
FN001 Base data
reg: 00000
```

To modify the base data register (00000 to 65535, use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Base Data Register Offset

Register Offset	Register Function
0	*Input Value Set Point* The input value set point is used to determine at what point the comparison input register value used in the calculation is high or low. The Input Hysterisis value is added or subtracted from the set point to prevent an oscillation on the output PGM's.
1	*Input Hysterisis Value* The hysterisis value that the comparison input must be above or below the setpoint to activate the low or high PGM outputs. This value is added to the input value or subtracted dependent on the direction the comparison input is changing.
2	*Input Hysterisis Time* The time that the value must be above or below the set point to proceed with activating the low and high PGM outputs. This setting is the number of seconds the value must be above or below.

Using the register configuration settings above and the following data values in the configuration registers the following will be observed. The comparison input register in this example is linked to the first channel on the Analog Expander. This was tested using a linear variable resistor with a 10V supply reference that can be connected to the input to allow manual control using the knob on the variable resistor.

Programmed Settings

Base Register is 00100

Value Data Register is 00000 (First Analog Input Channel on AE001)

Base Register Configuration

Register 00100 Input Set Point = 1200

Register 00101 Input Hysterisis = 100

Register 00102 Input Hysterisis Time = 20

Given the above settings and assuming that the data value for the input comparison is set to 0 when the programmable function is started after 20 seconds the low PGM (if it is set) will be activated. When the data value rises and exceeds the 1200 set point for longer than 20 seconds (Hysterisis Time) the low value will be deactivated. If the input then exceeds the set point plus the hysterisis value (1300) for longer than 20 seconds the high PGM will be activated and will deactivate when the input value is below the set point for longer than the 20 second time.

Setting a very low hysterisis time value can result in the system oscillating and causing unstable operation, it is recommended to have a reasonable value for these settings.

Daylight Sensor

For example a daylight sensor that can be used would be set to hysterisis of 250 and a time of 120 seconds, this ensures any variation in cloud cover, headlights or other scenarios are managed by the comparison function and would not cause the lights being controlled from either flicking off or on in a brief over/under light situation.

Comparison Input Register

The comparison input register is used for the source of the data to perform a comparison. For example using a register setting of 00000 would perform a comparison with the data being sent from Channel 1 of the first Analog Expander.

The comparison input register DOES NOT have to be a register that is linked with an analog expander. This can be a register that is controlled from the Protege System Management Suite or from another register. This is also an ideal method of testing the comparison function before putting it in to operation.

```
FN001 Comp inp
reg: 00000
```

To modify the comparison input register (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Ripple Control PGM Output Function

The ripple control function will activate and then deactivate in sequence the PGM's that are assigned to the stage outputs. Ideally suited for staging on lighting and air conditioning systems in large industrial sites.

```
FN001 Func Type
Ripple PGM
```

Use the [1] and [3] keys to scroll the function types until you reach the Ripple PGM selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the Value Compare function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

Setting the run once option for the ripple PGM function will result in NO operation being performed and the function stopping a short time after it is started.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to move to the next programmable option for the ripple PGM function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Enabled Control PGM

The Enabled Control PGM is used to operate the ripple PGM function in the STEP UP mode when it is activated and it will run in the STEP DOWN mode when the Enable PGM is deactivated. If no enabled PGM is set the function will never run the ripple stages.

```
FN001 Enabled
pgm: --000:00
```

To modify the enabled PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336). To select a data register press the stay key, the following screen will be shown and a memory register location can be selected. To view the memory register locations refer to appendix memory registers.

Ripple On Time

The ripple on time determines the time that each PGM output will be delayed before being activated when the ripple control function is stepping the PGM outputs up.

```
FN001 Ripple on
time: 00000 secs
```

To modify the ripple on time (00000 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Ripple Off Time

The ripple off time determines the time that each PGM output will be delayed before being deactivated when the ripple control function is stepping the PGM outputs down.

```
FN001 Ripple off
time: 00000 secs
```

To modify the ripple off time (00000 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Stage 1 PGM

The first PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 1
pgm: --000:00
```

To modify the Stage 1 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 2 PGM

The second PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 2
pgm: --000:00
```

To modify the Stage 2 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 3 PGM

The third PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 3
pgm: --000:00
```

To modify the Stage 3 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 4 PGM

The fourth PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 4
pgm: --000:00
```

To modify the Stage 4 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 5 PGM

The fifth PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 5
pgm: --000:00
```

To modify the Stage 5 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 6 PGM

The sixth PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 6
pgm: --000:00
```

To modify the Stage 6 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 7 PGM

The seventh PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 7
pgm: --000:00
```

To modify the Stage 7 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Stage 8 PGM

The eigth PGM in the 8 PGM outputs that can be programmed for the ripple control function.

```
FN001 Stage 8
pgm: --000:00
```

To modify the Stage 8 PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Door Control Function

To program the door control function ensure that the function you have selected is halted. Select the function type selection screen as shown below for Door Control.

```
FN001 Func Type
Door Control
```

Use the [1] and [3] keys to scroll the function types until you reach the door control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Door Action

The action determines what action is performed on the door or door group that is programmed as a result of the Input PGM. An action MUST be selected for the programmable function to operate correctly.

```
FN001 Action
None
```

Use the [1] and [3] keys to scroll the action types until you reach the required action that you want to be performed and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

- Follow and Test

The door status follows the programmed input one state and will retest the input state every 30 second interval and change the door state accordingly.

Input One	Door
ON	UNLOCKED
OFF	LOCKED

Test Action - If the door state is changed externally or is part of another programmable function the programmable function will only restore the output state after 30 seconds has elapsed. This time is only used if the programmable function was NOT responsible for the change in state. If a door has a door unlock time and the door mode is set to timed this will unlock the door every 30 seconds.

- Not Follow and Test

Performs the same function as above however the output is inverted (NOT). This logic action is a test action, consult the follow and test action for an explanation of the Test Function.

Input One	Output
ON	LOCKED
OFF	UNLOCKED

- Pulse On

The pulse on action will unlock the door only when the input one has transitioned from an off to an on state. The door will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output
	UNLOCKED

- Not Pulse On

The not pulse on action will lock the door only when the input one has transitioned from an off to an on state. The door will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	LOCKED

- Pulse Off

The pulse on action will unlock the door only when the input one has transitioned from an ON to an OFF state. The door will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output
	UNLOCKED

- Not Pulse Off

The not pulse off action will unlock the door only when the input one has transitioned from an ON to an OFF state. The output will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	LOCKED

Input One PGM

Input one selects the input source to the door control process that is being configured. All door control functions use at least one input source. Input one must be programmed with a valid input source, if an input source is selected that is not valid when the function is started an error will be generated and the function suspended. An input source can be a PGM (Programmable Output).

```
FN001 Input one
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Control Door

The control door selects the door to control as a result of the action being performed by the programmable function. To control a door group leave the control door option set to none and proceed to the Control Door Group entry screen. Selecting both a door and a door group will result in only the door being controlled and the door group being ignored.

```
FN001 Door
None
```

Use the [1] and [3] keys to scroll the action types until you reach the door that you want to control and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Control Door Group

The control door group selects the area group to control as a result of the action being performed by the programmable function. To control a door leave the control door group set at none and program a door in the control door section. Programming a door and a door group will result in the door group not being used.

```
FN001 Door Grp
None
```

Use the [1] and [3] keys to scroll the door groups until you reach the required group and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Door Control Mode

The control mode selects how the door will be controlled in the control door or control door group setting. This allows a door to be unlocked for the door unlock time, unlock latched or unlocked in the fire alarm mode.

```
FN001 Door Mode
Menu Timed
```

Use the [1] and [3] keys to scroll the door control mode until you reach the setting that you want to use and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Door Mode	Description
Menu Timed	The Door will be unlocked for the door unlock time that is programmed for the door. Use this mode when you want to unlock the door for unlock time. The door will lock after the unlock time has expired.

Door Mode	Description
Menu Latched	The door will be latched in the unlocked state and will remain unlocked until controlled from: ▸ A LCD Keypad ▸ Protege System Management Suite ▸ Scheduled Action ▸ Area Status ▸ A Programmable function.
Fire Control	The door will be latched in the fire control unlock state and will remain unlocked until controlled from: ▸ A LCD Keypad ▸ Protege System Management Suite ▸ A Programmable function that is programmed to deactivate the fire alarm control.
Lockdown	Door Lockdown will be started for the door or door group and will remain Protege an LCD Keypad or when the PGM input goes off if the function is operating in a Test and Follow mode.
Lockdown (Entry Allowed)	Door Lockdown with Entry Allowed will be started for the door or door group and will remain locked down until it is cancelled from the Protege System Management Suite, an LCD Keypad or when the PGM input goes off if the function is operating in a Test and Follow mode.
Lockdown (Exit Allowed)	Door Lockdown with Exit Allowed will be started for the door or door group and will remain locked down until it is cancelled from the Protege System Management Suite, an LCD Keypad or when the PGM input goes off if the function is operating in a Test and Follow mode.
Lockdown (Entry and Exit Allowed)	Door Lockdown with Entry and Exit Allowed will be started for the door or door group and will remain locked down until it is cancelled from the Protege System Management Suite, an LCD Keypad or when the PGM input goes off if the function is operating in a Test and Follow mode.

Virtual Door Function

To program the virtual door function ensure that the function you have selected is halted. Select the function type selection screen as shown below for the Virtual Door.

```
FN001 Func Type
Virtual Door
```

Use the [1] and [3] keys to scroll the function types until you reach the door control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Rex Zone Input

The Request to Exit (REX) Input is connected to the Virtual Door's REX Zone. When this zone is closed the Lock PGM is activated and the door can be opened for the Max Open time when no alarms being generated.

This zone should be configured as a digital zone, therefore disable the "EOL Resistor on zone input" option. If a Normally Closed REX button is used the zone should inverted option should be set for the zone to ensure pushing the button will generate the REX event.

This zone must also be placed in an armed area for the Virtual Door to operate.

```
FN001 REX

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Door State Zone Input

The Door Position input is connected to the Door State Zone. This should be configured so that when the door opens the zone opens. It may be necessary to invert the zone input to ensure this operation.

This zone should be configured as a digital zone, therefore disable the "EOL Resistor on zone input" option.

This zone must also be placed in an armed area for the Virtual Door to operate.

```
FN001 Door State

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Virtual Door Left Open Zone

When programmed this zone is controlled by the Virtual Door Function such that when the door is left open longer than the Max Open time and a Door Left Open event is generated this zone will be opened. When the door closes, the zone will also close. Place this zone in a reportable area to enabled reportable events from the virtual door.

```
FN001 Left Open

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Virtual Door Forced Open Zone

When programmed this zone is controlled by the Virtual Door Function such that when the door is forced open and a Door Forced Open event is generated this zone will be opened. When the door closes, the zone will also close. Place this zone in a reportable area to enabled reportable events from the virtual door.

```
FN001 Forced

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Virtual Door Unlock Time

The unlock time determines how long the lock that controls the virtual door will remain unlocked for when a user access's the door.

```
FN001 Unlock
time: 005 secs
```

To modify the unlock time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a 000 value will result in the door not unlocking when a users access's the door.

Virtual Door Maximum Open Time

The maximum open time is programmed to allow the door to be left open for a certain period before it will generate a door left open condition. When the left open condition is reached this will activate the alarm PGM and open the left open zone.

```
DR001 Pre-Alarm
time: 030 secs
```

To modify the pre-alarm time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting a 000 value will result in the pre-alarm feature not operating.

Virtual Door Lock PGM or PGM Group

You can assign a PGM or PGM group that controls the physical electric lock for the door.

```
FN001 Door Lock
pgm: --000:00
```

To modify the door lock PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Alarm PGM or PGM Group

You can assign a PGM or PGM group that will activate when the door goes into either a left open or forced condition. Use this to warn the user to close the door. See miscellaneous options below for configuring how the PGM is activated.

```
DR001 Pre Alarm
pgm: --000:00
```

To modify the pre alarm PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Virtual Door Miscellaneous Options

These options are for the virtual door.

Option 1 – Alarm on Door Left Open

- The Alarm PGM will be activated when the door is left open beyond the Max Open time.
- The Alarm PGM is not activated.

Option 2 – Pulse Left Open Alarm

- The Alarm PGM will be activated with a pulse time on and off.
- The Alarm PGM will be turned on normally.

Option 3 – Alarm on Door Forced

- The Alarm PGM will be activated when the door is forced open.
- The Alarm PGM is not activated.

Option 4 – Pulse Forced Door Alarm

- The Alarm PGM will be activated with a pulse time on and off.
- The Alarm PGM will be turned on normally.

Option 5 – Log Left Open Zone Event

- Enabled the zone events when the door is left open.
- Disables the zone events from being generated.

Option 6 – Log Forced Zone Event

- Enabled the zone events when the door is forced open.
- Disables the zone events from being generated.

Option 7 and 8 - Reserved

- Reserved do not modify

Zone Follows PGM Function

To program the zone follows pgm function ensure that the function you have selected is halted. Select the function type selection screen as shown below for Zone Control.

```
FN001 Func Type
Zone Control
```

Use the [1] and [3] keys to scroll the function types until you reach the door control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Control Zone

The control zone's state will be set to be opened or closed according to the start of the Control PGM. If the PGM is OFF the zone will be closed. If the PGM is ON, TIMED ON or PULSED ON the zone will be open. The zone must be placed in an armed area to use it for control or reporting.

```
FN001 Control

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Control PGM

The Control PGM's state will be followed by the Control Zone.

```
FN001 Control

pgm: CP001:01
Halted
```

To modify the Control PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Miscellaneous Options

These options are for the function.

```
FN001 Misc

   [1--------]
Halted
```

Option 1 – Log Zone Events

- Enable Zone events when the zone changes state.
- Disable any Zone Events.

Option 2 - 8 – Reserved

- Reserved do not modify

Elevator Control

To program the Elevator Control function ensure that the function you have selected is halted. Select the function type selection screen as shown below for Elevator Control.

```
FN001 Func Type
Elevator Ctrl
```

Use the [1] and [3] keys to scroll the function types until you reach the door control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the elevator control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the elevator control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Elevator Action

The action determines what action is performed on the elevator group that is programmed as a result of the Input PGM. An action MUST be selected for the programmable function to operate correctly.

```
FN001 Action
None
```

Use the [1] and [3] keys to scroll the action types until you reach the required action that you want to be performed and then press [ENTER] to proceed to the next programmable option for the elevator control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

- Follow and Test

  The floor group status follows the programmed input one state and will retest the input state every 30 second interval and change the floor group state accordingly.

Input One	Floor Group
ON	UNLOCKED
OFF	LOCKED

  Test Action - If the floor group state is changed externally or is part of another programmable function the programmable function will only restore the output state after 30 seconds has elapsed. This time is only used if the programmable function was NOT responsible for the change in state. If a door has a door unlock time and the door mode is set to timed this will unlock the door every 30 seconds.

- Not Follow and Test

  Performs the same function as above however the output is inverted (NOT). This logic action is a test action, consult the follow and test action for an explanation of the Test Function.

Input One	Output
ON	LOCKED
OFF	UNLOCKED

- Pulse On

  The pulse on action will unlock the floor group only when the input one has transitioned from an off to an on state. The floor group will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output
	UNLOCKED

- Not Pulse On

  The not pulse on action will lock the door only when the input one has transitioned from an off to an on state. The door will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	LOCKED

- Pulse Off

  The pulse on action will unlock the floor group only when the input one has transitioned from an ON to an OFF state. The floor group will not be modified further from this state and will not be modified if it is turned OFF by another function.

Input One	Output

	UNLOCKED

- Not Pulse Off

  The not pulse off action will unlock the floor group only when the input one has transitioned from an ON to an OFF state. The output will not be modified further from this state and will not be modified if it is turned ON by another function.

Input One	Output
	LOCKED

Input One PGM

Input one selects the input source to the elevator control process that is being configured. Input one must be programmed with a valid input source, if an input source is selected that is not valid when the function is started an error will be generated and the function suspended. An input source can be a PGM (Programmable Output).

```
FN001 Input one
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Elevator Group

The elevator group selects the elevators to control as a result of the action being performed by the programmable function.

```
FN001 Elev Grp
None
```

Use the [1] and [3] keys to scroll the action types until you reach the elevator group that you want to control and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Floor Group

The floor group selects the floors that will be activated on all of the elevators in the elevator group as a result of the action being performed by the programmable function.

```
FN001 Floor Grp
None
```

Use the [1] and [3] keys to scroll the floor groups until you reach the required group and then press [ENTER] to proceed to the next programmable option for the elevator control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Token Unlock Time

The token unlock time is the period of time the floor group will be activated for as a result of the action by the programmable function.

```
FN001 Token
time: 010 secs
```

Elevator Control Mode

The control mode selects how the floor group will be controlled. This allows a door to be unlocked for the token time, unlock latched or unlocked in the fire alarm mode.

```
FN001 Door Mode
Menu Timed
```

Use the [1] and [3] keys to scroll the door control mode until you reach the setting that you want to use and then press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Door Mode	Description
Menu Timed	The Floor Group will be unlocked for the token time that is programmed for the programmable function. Use this mode when you want to unlock the door for defined time. The floors will lock after the token time has expired.
Menu Latched	The floors will be latched in the unlocked state and will remain unlocked until controlled from: ▸ A LCD Keypad ▸ Protege System Management Suite ▸ Scheduled Action ▸ Area Status ▸ A Programmable function.
Fire Control	The door will be latched in the fire control unlock state and will remain unlocked until controlled from: ▸ A LCD Keypad ▸ Protege System Management Suite ▸ A Programmable function that is programmed to deactivate the fire alarm control.

Register Counter

To program the register counter function ensure that the function you have selected is halted. Select the function type selection screen as shown below for Register Counter.

```
FN001 Func Type
Reg Counter
```

Use the [1] and [3] keys to scroll the function types until you reach the door control selection and press [ENTER] to select the function type displayed and proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Func Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the door control function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Miscellaneous Options

These options are for the function.

```
FN001 Misc

   [1--------]
Halted
```

Option 1 – Increment on Zone Open

- Enable the counter will increment when the zone opens (alarm).
- Disable.

Option 2 – Increment on Zone Close

- Enable the counter will increment when the zone closes (seal).
- Disable.

Option 3 – Log Counter Events

- Enable the function will log an event for every increment.
- Disable.

Option 4 – Decrement on Zone Open

- Enable the counter will decrement when the zone opens (alarm).
- Disable.

Option 5 – Decrement on Zone Close

- Enable the counter will decrement when the zone closes (seal).
- Disable.

Option 6 – No Overflow on Register

- Enable the counter will not overflow (or underflow) when the register reaches 65535 counting up and 0 when counting down.
- Disabled the register will wrap around to 0 when incremented past 65535 and will wrap around to 65535 when decremented past 0.

Option 7, 8 – Reserved

- Reserved do not modify

Control Zone

The control zone will increment the counter register based on the options selected above.

```
FN001 Control

Zone CP001:01
Halted
```

To modify the input Zone, use the settings as explained in section Entering Zones (see page 337).

Counter Register

Enter the Register that will be incremented by the zone. The actual value of the counter is calculated as (Overflow Register * 65565) + Counter Register.

```
FN001 Counter
reg: 00100
```

Overflow Register

Enter the Register that will be incremented when the Counter register overflows.

```
FN001 Overflow
reg: 00101
```

Reset PGM

The counter and overflow registers are set to zero when this PGM activates. When this occurs and event is logged with the total before the reset occurs. The counter cannon be reset by a PGM group.

```
FN001 Reset
pgm: --000:00
```

To modify the input PGM, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Average

The average function takes the average of up to eight input registers and writes this to an output register.

To program the Average function ensure that the function you have selected is halted. Select the function type selection screen as shown below for the Average function.

```
FN001 Fnc Type
Average
```

Use the [1] and [3] keys to scroll the function types until you reach the desired function and press [ENTER] to select this and proceed to the next programmable option. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Fnc Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the Average function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Input Registers

Select up to eight Input registers. If a valid register number is entered it will be used as part of the Average calculation. If an invalid register number is selected (eg. 65535) then it will not be used as part of the calculation.

```
FN001 Input #1
reg: 00001
```

...

```
FN001 Input #8
reg: 65535
```

To modify the Input registers (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Output Register

Select a register to which the output will be written.

```
FN001 Output
reg: 65535
```

To modify the Output register (00000 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Update Time

Select an Update time. This is the number of seconds between the update of the output register.

```
FN001 Update
time: 00005 secs
```

To modify the Update time (00001 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Output Compare

The output compare function will take an input *variable* and scan an input *profile* to select an *output* value which is then written to an output register. The input register can be any valid register. The input profile is defined as a range of up to 32 Compare Registers. These registers contain a series of values. The input value is compared with each compare value, starting from the first one, and if a match is found the corresponding output value is copied to the output register. A match is found when the Input value lies between the values of one compare register and the next. The output associated with the compare value that is closest to the input value is then copied to the output register.

To program the Output Compare function ensure that the function you have selected is halted. Select the function type selection screen as shown below for the Output Compare function.

```
FN001 Fnc Type
Output Compare
```

Use the [1] and [3] keys to scroll the function types until you reach the desired function and press [ENTER] to select this and proceed to the next programmable option. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Function Mode

The function mode determines how this function operates with the system controller. By default a function is set to normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will allow the function to run once and then wait to be stopped and started by the user or operator.

```
FN001 Fnc Mode
Normal
```

Use the [1] and [3] keys to scroll the function mode until you reach the normal selection and press [ENTER] to proceed to the next programmable option for the Output Compare function. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Input Register

This the Register which contains the Input value which gets compared to the profile. It would typically be assigned to a physical analogue input module.

```
FN001 Input
reg: 00001
```

To modify the Input register (00001 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Output Register

This is the register to which the output is directed. It would typically be assigned to a physical analogue output module.

```
FN001 Output
reg: 00001
```

To modify the Output register (00001 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Compare Register Base

This is the first register in a sequence of registers which will contain the values to which the input is compared.

```
FN001 Comp base
reg: 00001
```

To modify the base Compare register (00001 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Output Register Base

For every compare value register there must be an output value register. If the input matches the compare value then the corresponding output value is copied to the out put register.

```
FN001 O/P base
reg: 00001
```

To modify the base Output register (00001 to 65535), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Number of Points

This defines the number of registers starting from the Compare Register Base which will be checked as the input profile.

```
FN001 Number of
points: 004
```

To modify the Number of Points (001 to 032), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Update Rate

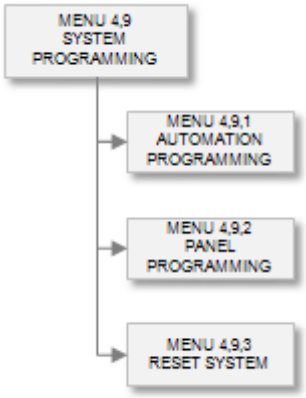
Select an Update time. This is the number of seconds between the update of the output register.

```
FN001 Update
time: 00005 secs
```

To modify the Update time (00001 to 65535 seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

General Programming

The general programming menu contains programmable options for the automation PGM's and the panel configuration options. The restart menu [MENU, 4, 9, 3] allows the system controller to be restarted.



A panel restart is required for the TCP/IP address change to take affect once programmed in the panel configuration menu. The panel will remain operational on the previously assigned IP address until it is restarted.

To go to the general menu select [MENU, 4, 9]. You can then select from the menu items presented or scroll the menu using the [🡅] and [🡇] keys.

Automation

To access the automation programming login using a valid installer code and then select [MENU, 4, 9, 1]. The screen displays "Automation to modify" as shown in the following example.

```
Automation to
modify: AT001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the automation settings in the Protege System allow you to configure the automation that is shown on the system keypads.

Selecting an Automation Entry to Modify

Each automation entry is assigned a unique automation number from 001 to 250.

```
Automation to
modify: AT001
```

Type the appropriate 3-digit automation number or use the [🡇] and [🡅] keys to scroll the available automation entries. When the desired automation number appears on the screen, press [ENTER] to program the selected automation entry. The maximum number of automation outputs that can be programmed is limited by your system's memory and configured profile.

Automation Name

If the selected automation entry has a name associated (some automation entries may not have a name associated with them) the name programming screen will be shown.

```
AT001 Name
*Automation 001
```

To scroll automation entries by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected automation item use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the automation name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Automation PGM

The automation entry will control the PGM or PGM group that is assigned to the control PGM option.

```
AT001 Control
pgm: --000:00
```

To modify the automation PGM or PGM Group, use the settings as explained in section Entering PGM and PGM Groups (see page 336).

Automation PGM Activation Time

You can override the programmed activation time for a PGM or the group of PGM's by setting an activation time.

```
AT001 PGM on
time: 00000 secs
```

To modify the PGM on time (00000 to 65535 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Automation Clipsal C-Bus Application Number

The Clipsal C-Bus application number is used to link this automation point to a C-Bus Application that is communicating with the system controller via a PRT-COMM and Serial Communications Interface. For example if you want to link this automation point to activate when a Lighting, Switching and Load Control application command is generated for a particular Group Address set the Application Type to 056 (056 or $38 Hex is the Lighting, Switching and Load Control application, refer to the *Clipsal C-Bus Application Specifications* and related documents.

```
AT001 C-Bus App
type: 000
```

To modify the C-Bus Application type enter a value (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Automation Clipsal C-Bus Group Address

The Clipsal C-Bus group address is the number used to identify the group within the C-Bus network. This typically ranges from 0-255. A group allows any PGM in the Protege System to either control a C-Bus group as the result of a change within the system or to change based on a C-Bus group being activated. For example when a user press's a Goodbye Button on a C-Bus keypad this can activate a PGM that is used to ARM an Area in the Protege System. The PGM's can also be used to allow doors to Unlock/Lock based on the C-Bus events that occur.

```
AT001 C-Bus Grp
address: 000
```

To modify the C-Bus Group Address enter a value (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Automation Options

Automation options include inverted display and C-Bus automation options. For C-Bus to operate correctly a Protege PRT-COMM and Clipsal C-Bus PCI interface is required and the C-Bus service must be configured and started.

```
AT001 Control
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Automation Display Inverted

- Enabled the Automation display will show the automation status as inverted. Set this option when a PGM or PGM Group operates inverted to the normal state.
- Disabled the Automation will display in the normally open state.

Option 2 – Enable C-Bus Automation Functions

- Enabled the Automation point will be included in the C-Bus processing and used to control or be controlled by a C-Bus automation point.
- Disabled the Automation point is not used for C-Bus.

Option 3 - C-Bus Automation Output

- Enabled the Automation point will generate a C-Bus message on the C-Bus system when the status of the Automation point changes. For example manually controlling the Automation point will send the Application Id and Group Address to the C-Bus interface.
- Disabled the Automation point is will be updated based on the C-Bus message and group. For example if this option is disabled and a C-Bus message is received that match's the programmed settings the automation point will activate the PGM.

Option 4 – Use PGM Status In C-Bus Functions

- Enabled the Automation point will use the programmed PGM directly rather than using the automation point status or setting. This allows any PGM in the system to be programmed for the automation point without it actually being controlled by the automation point.
- Disabled the Automation point status will be used for C-Bus operations.

Option 5 – C-Bus Functions Operate On Rising Edge

- Enabled the C-Bus processing will only activate on the rising edge of a change in the Automation Point or PGM state. For example the Automation point changing from Off to On.
- Disabled the C-Bus processing will ignore any change from Off to On.

Option 6 – C-Bus Functions Operate On Falling Edge

- Enabled the C-Bus processing will only activate on the falling edge of a change in the Automation Point or PGM. For example the Automation point changing from On to Off.
- Disabled the C-Bus processing will ignore any change from On to Off.

Option 7 and 8 - Reserved

- Reserved do not modify

Panel Configuration

The panel configuration allows hardware settings to be programmed in to the system controller that affect the way it operates and functions. To access the panel configuration programming login using a valid installer code and then select [MENU, 4, 9, 2]. The screen displays the first entry to modify as there is only one panel no record selection is required. The first item that is programmable is the AC Failure time as shown in the following example.

```
AC Failure
time: 030 secs
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the panel settings in the Protege System allow you to configure the hardware. Some settings that are programmable require that a service that uses the setting is restarted (for example changing the TCP/IP Address requires that the TCP/IP service is restarted).

AC Failure Time

The AC Failure time allows the installer to program a time that AC mains voltage must have failed before activating the AC Failure Trouble Zone. Set this to a larger value for locations that experience frequent but short interruptions in power or that operates on a generator frequently.

```
AC Failure
time: 030 secs
```

To modify the AC Failure time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

AC Restore Time

The AC Restore time allows the installer to program a time that AC must be present for after a AC Failure before restoring the AC Failure Trouble Zone. Set this to a larger value for locations that experience frequent but short interruptions in power or that operates on a generator frequently.

```
AC Restore
time: 030 secs
```

To modify the AC Restore time (000 to 255 Seconds), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Battery Test Time

The battery test time allows the installer to program the duration of time in minutes between each battery test that is performed. A battery test is performed immediately on power up of the panel and then every programmed period. Each battery test takes 45 seconds and the battery low/failure trouble zone will activate if the battery fails.

```
Battery Test
Time: 015 mins
```

To modify the Battery Test time (000 to 255 Minutes), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Default LCD Text Line One

The default LCD text for line one is shown on all PRT-KLCD keypads when they are first connected to the system. This text should be changed to the name of the building, installation or owners details. To view the information on setting the time, date or other variable text see the formatting character information in the following section.

```
Def LCD Line 1
 Protege System
```

To modify or enter a new name for the selected default LCD line item use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

Default LCD Text Line Two

The default LCD text for line two is shown on all PRT-KLCD keypads when they are first connected to the system. This text should be changed to the name of the building, installation or owners details.

```
Def LCD Line 2
     By ICT
```

To modify or enter a new name for the selected default LCD line item use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

The default text can also display variable text information such as the time, date and temperature. These are called formatting characters and all are prefixed with the '&' sign. For example to display the time, day and month on the bottom line of the default message for the LCD program the following information.

Set the text for line one to the company name, building name or other informative information.

```
Def LCD Line 1
 AB Corporation
```

Program the time and date formatting characters in to the default display for Line 2 as shown below.

```
Def LCD Line 2
 &T      &D &V
```

The above setting will display the time in standard 12 hour format with the AM and PM indicators in lower case, then the day of the month followed by the three letter abbreviation for the month.

The display that will be shown on the keypad would be shown as follows:

```
 AB Corporation
 10:18am 19 Sep
```

A large number of formatting characters allow the customization of the display to show many different variations depending on customer requirements. The currently available formatting characters are shown in the following table.

Character	Function
T	Show the time in 12 hour format with the am/pm symbol in upper case following the time. Example 11:02PM.
t	Show the time in 12 hour format with the am/pm symbol in lower case following the time. Example 11:02am.
M	Show the time in 24HR (Military Format) with a leading space for numbers below 10 hours. Example 9:00
m	Show the time in 24HR (Military Format) with a leading zero for numbers below 10 hours. Example 09:00
G	Show the time in 12 hour format with leading spaces and no am/pm symbol. Example 11:02.

Character	Function
A	Show the AM/PM symbol in uppercase. Example PM.
a	Show the AM/PM symbol in lowercase. Example pm.
D	Show the day of the month. Example 9 or 18 a leading space is used for all numbers below 10.
V	Show the month in an abbreviated 3 characters. Example Jan or Nov.
v	Show the month in 2 character format. Example 4 or 12 a leading space is used for all numbers below 10.
s	Show the month in 2 character format. Example 04 or 12 a leading zero is used for all numbers below 10.
R	Show the day of the week in abbreviated 3 characters. Example Mon or Fri.
Y	Show the year with leading zeros. Example 05.
C	Show the century. Example 20 or 19.
K	Show the temperature from the local temperature sensor on the LCD keypad in Degrees Celsius. Example 22.5°C. This will be updated from the LCD keypads temp sensor.
k	Show the temperature from the local temperature sensor on the LCD keypad in Degrees Fahrenheit. Example 76.5°f. This will be updated from the LCD keypads temp sensor.

Panel Name

The panel name is programmed to identify the panel to the operator or system user. Ideally should describe the name of the premises or the building where the panel is installed. The panel name is also used within the IP and SMTP Mail Services to identifiy the panel to the e-mail recipient.

```
Panel Name
PROTEGE
```

To modify or enter a new name for the panel use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

Panel Network Address

The panel network address sets the address that the system controller will communicate when connected using RS485 communications. This allows multiple panels to be connected using a single RS-485 Serial Communications Interface.

When connecting with TCP/IP this address should be programmed as 000 as the TCP/IP address will be used to identify this unit.

```
Panel network
Address: 000
```

To modify the panel network address (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting an address of 255 will disable the communication.

Panel IP Address

The system controller has a built in TCP/IP Ethernet Device and it must be programmed with a valid TCP/IP Address to allow the software to connect. By default the IP address is set to 192.168.1.2.

Programming a IP address requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

```
IP Address
192.168.001.002
```

To modify the panel IP address use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting an address of 255 will disable the communication.

Panel IP Netmask

In conjunction with the IP Address a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to a value of 255.255.255.0.

Programming a IP Netmask requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

```
IP Address
255.255.255.000
```

To modify the panel IP netmask use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting an address of 255 will disable the communication.

Panel IP Gateway

In conjunction with the IP Address a gateway can be configured to allow access to a router for external communications beyond the subnet to which the system controller is connected. By default this is set to a value of 0.0.0.0 to prevent any external communication.

Programming a IP Gateway requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

```
IP Gateway
000.000.000.000
```

To modify the panel IP gateway use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. Setting an address of 255 will disable the communication.

Panel Upload ID

The panel upload ID is used as a security key in combination with the host verify ID for communication with the Protege System Management Suite. The upload and host ID keys prevent the remote connection of a Protege System Management Suite other than that which has the same 32 bit keys.

```
Panel upload
ID: 00000000
```

To modify the panel upload id, use the keypad as explained in section Entering Hexadecimal Numbers (see page 335) and press [ENTER].

Host Verify ID

The host verify ID is used as a security key in combination with the panel upload ID for communication with the Protege System Management Suite. The upload and host ID keys prevent the remote connection of a Protege System Management Suite other than that which has the same 32 bit keys.

```
Host verify
ID: 00000000
```

To modify the host verify id, use the keypad as explained in section Entering Hexadecimal Numbers (see page 335) and press [ENTER].

Module UDP Port

This is the UDP port that all Ethernet enabled modules will communicate with the Protege System Controller over. If this port is changed all modules will need to also be changed.

Panel Options

Panel options include configuration settings that affect the test report trouble zone, login and security parameters as well as the operation of certain panel hardware devices.

```
Panel Options
   [-2-----8]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - High Current Battery Charging

- Enabled the system controller will set the charge current to 750mA.
- Disabled the system controller will set the charge current to 350mA.

Option 2 - Generate Test Report by Time of Day

- Enabled the test report trouble zone will be activated at a specific time of day. For example, if the Test Report setting is set to 02:00 then the trouble zone will be activated at 2:00am each morning.
- Disabled the test report trouble zone will be activated periodically. For example, if the Test Report setting is set to 00:15 then the trouble zone will be activated every 15 minutes.

Option 3 - Trouble Condition Require Acknowledge

- Enabled any trouble condition will be latched and remain active until a user logs in the keypad and acknowledges the trouble condition.
- Disabled the system controller will automatically clear the trouble condition when the trouble has been cleared.

Option 4 - Reserved

- Reserved do not modify

Option 5 - Generate Trouble Zone Test Report Restore

- Enabled the system controller will generate a restore event for the trouble zone test report zone restoring. This occurs one minute after the trouble zone has been activated.
- Disabled the system controller will not generate a restore.

Option 6 - Log Zone Reference Updates

- Enabled the system controller log zone reference changes that it performs as a result of calculations that it performs periodically to ensure a high level of system integrity.
- Disabled the system controller will not log the events.

Option 7 - Log Operating System Assertion Events

- Enabled the system controller will log operating system assertion events that occur. An assertion event is generating when the system controller gets a value, command or performs a function that results in a condition that is not deemed normal.
- Disabled the system controller will not log operating system assertion events.

Option 8 - Remote Login Not Required

- Enabled the system controller will not validate the login and user name that is provided from the remote Protege System Management Suite or other remote host systems that must log in to the system.
- Disabled the system controller will require that any external host accessing the system uses a valid login and user id number to gain access.

Miscellaneous Options

Miscellaneous options include configuration settings that affect the offline functions and remote intelligent door reader operations.

```
Misc Options
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 – Auto Update Offline Users

- Enabled the system controller will automatically update offline configuration parameters to all RDI modules at the time programmed in the Offline User Update Time.
- Disabled the system controller will take no action for offline users.

Option 2 – Use Alternate Resistors

- Enabled the system controller will use alternate EOL configured resistors (2K2 and 6K8).
- Disabled the system controller will use the normal 1K and 1K resistor configuration.

Option 3 – Invert Module Tamper

- Enabled the system controller will invert the module tamper input allowing a normally open (door closed) tamper switch to be used.
- Disabled the system controller will use the standard normally closed (door closed) tamper switch.

Option 4 - Reserved

- Reserved do not modify

Option 5 - Reset Anti-Passback Status On schedule

The anti-passback status of all users can be reset on schedule. This flag will enable this global function. The associated 'Anti-Passback reset schedule' must also be set correctly for this option to function.

Option 6 - Enable Timed User Anti-Passback Reset

A specific time for Entry and Exit anti-passback can be set under the Door options to block a user from passing through a door too often. The time can be individually specified per Door but is globally enabled using this option flag.

Anti-pass back Reset Schedule

If the 'reset anti-passback status on schedule' option has been selected (misc option 5) then all users will have their anti-passback status reset when the specified schedule becomes valid.

```
AntiPass Rst Sch
*Schedule 001
```

Use the [1] and [3] keys to scroll the schedule selection and press [ENTER] to select the schedule displayed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Register Onboard Reader

The onboard reader functions in the same manner as any other reader expander module and needs to register at a specific address. This option allows you to define what that address is.

```
Panel Rdr addr
008
```

To modify the Onboard reader address (001 to profile maximum), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER]. A value of 255 will disable the Onboard Reader.

Onboard Reader Door Locks

The onboard reader can be configured to use the Panel Bell outputs (CP PGM 1 & 2), the Panel PGM outputs (CP PGM 3 & 4) or no Panel outputs for it's Door lock PGMs. Note that this setting only applies if, under the Door set up for the doors accessed by the onboard reader, the lock PGMs are specified as the lock PGMs for that reader (the default setting).

```
Panel Rdr o/p
Panel Bells
```

Use the [1] and [3] keys to scroll the Output setting and press [ENTER] to select the desired output. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Test Report Time

The test report time in conjunction with option 2 sets the time of the day or the period that the test report trouble zone activates. When option 2 is disabled the time programmed will be used as a period between reports in hours and minutes.

```
Test report
time: 02:00
```

To modify the test report time (00:00 to --:--), use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER]. Setting a test report time of --:-- will disable the activation of a test report.

Automatic Offline User Update Time

The automatic user offline update time in conjunction with option 1 in the miscellaneous options allows the panel to update the users and other offline parameters on all intelligent modules at a set time of the day.

```
Offline update
time: 03:00
```

To modify the offline update time (00:00 to --:--), use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER]. Setting an offline update time of --:-- will disable the offline user update function.

Modem Country Selection

The onboard modem must be configured for the region that the System Controller is being installed in to ensure proper operation.

```
Modem Country
NZ/Aus
```

Use the [1] and [3] keys to scroll the modem country selection until reach the required country and press [ENTER] to proceed. For more information about list control data entry refer to the section List Control Data Entry (see page 335).

Default Panel Language

The System Controller supports multiple languages on the Keypad and the Serial Event Printers. The language selected here will be the default language for users who have no language selected and also for any events.

```
Language
English
```

Use the [1] and [3] keys to scroll through the language selection until you reach the required language and press [ENTER] to proceed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

System Controller Restart

To access the system controller restart menu select [MENU, 4, 9, 3]. The screen will immediately prompt "Press [ENTER] to restart panel".

Pressing the [ENTER] key will restart the panel. The keypad that is currently being used will be restarted and will go offline for a short period of time while the panel restarts. This is part of normal operation for a panel restart.

```
Press [ENTER] to
restart panel.
```

If a panel restart is not required press the [MENU] key to exit and remain logged in or press the [CLEAR] key to exit and logout.

System Controller Restart in Bios Mode

On the Protege System Controller, Ensure Dip switch 2 is ON

Cycle the power to the Module.

To access the system controller restart menu select [MENU, 4, 9, 4]. The screen will immediately prompt "Press [ENTER] to restart panel".

Pressing the [ENTER] key will restart the panel in bios mode, which allows firmware updates to be performed. The keypad that is currently being used will be restarted and will go offline for a short period of time while the panel restarts. This is part of normal operation for a panel restart.

```
Press [ENTER] to
restart panel.
```

If a panel restart is not required press the [MENU] key to exit and remain logged in or press the [CLEAR] key to exit and logout.

Custom Reader Format

The Protege System Controller and Protege Reader Expansion Modules can support custom Wiegand Card Reader formats for the times when the format required is not one of the many available preset formats.

One custom format can be added per controller and used by any reader expander in the system.

Interface Type

To access the custom reader format programming login using a valid installer code and then select [MENU, 4, 9, 5]. The screen displays the first entry to modify as there is only one panel no record selection is required. The first item that is programmable is the output format.

The data can either be output as Wiegand (D0 and D1) or Magnetic Data (Clock and Data).

```
CF001 Type
Wiegand
```

Use the [1] and [3] keys to scroll the format type until you reach the required format and press [ENTER] to proceed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Data Length

The data length defines the total number of bits that are sent by the card reader for each card badge.

```
CF001 Length
bits: 026
```

To modify the length (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Facility Code Start

The facility code start defines the index where the facility code data starts in the data transmitted. The count starts at zero.

```
CF001 Site Start
bits: 001
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Facility Code End

The facility code end defines the index where the facility code data ends in the data transmitted. The count starts at zero.

```
CF001 Site End
bits: 008
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Card Number Start

The card number start defines the index where the facility code data starts in the data transmitted. The count starts at zero.

```
CF001 Card Start
bits: 009
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Card Number End

The card number end defines the index where the facility code data end in the data transmitted. The count starts at zero.

```
CF001 Card End
bits: 024
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Data Type

The data type defines how the card number that is received from the card reader is handled. If the size of the facility code and card number are less than 16 bits (e.g. Facility Start – Facility End is less that 16 bits) use 16 bit, otherwise use 32 bit. If unsure use 32 bit.

```
CF001 Data Type
16 Bit
```

Use the [1] and [3] keys to scroll the data type until you reach the required type and press [ENTER] to proceed. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Parity Location Block 1 to 4

There can be up to 4 blocks of parity calculated over the received data. They are all programmed using the same method and therefore the manual only covers programming the first block of parity (Parity 1).

The parity location defines where the location of the parity bit in the received data. The count starts at zero. If there is no parity set this value to 255.

```
CF001 Par1 Loc
bit: 000
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Parity Start Block 1 to 4

The parity start defines where the location of the parity block starts in the received data. The count starts at zero. If there is no parity set this value to 255.

```
CF001 Par1 Start
bit: 001
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Parity End Block 1 to 4

The parity start defines where the location of the parity block ends in the received data. The count starts at zero. If there is no parity set this value to 255.

```
CF001 Par1 End
bit: 012
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Parity Type Block 1 to 4

The parity type defines the method of calculating the parity for the block. This is either Even or Odd Parity.

```
CF001 Par1 Type
Odd Parity
```

Use the [1] and [3] keys to scroll the parity type until you reach the required type and press [ENTER] to proceed. For more information about the list control data entry refer to the section List Control Data Entry. (see page 335)

Parity Set Bit 1 to 4

There can be up to 4 defined set bits in the received data. A set bit defines a location in the received data that must always be set (or a logical '1'). They are all programmed using the same method and therefore the manual only covers programming the first set bit.

The set bit defines where the location of the bit in the received data. The count starts at zero. If there is no set bit this value to 255.

```
CF001 Set Bit 1
bit: 255
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

Parity Clear Bit 1 to 4

There can be up to 4 defined clear bits in the received data. A clear bit defines a location in the received data that must always be cleared (or a logical '0'). They are all programmed using the same method and therefore the manual only covers programming the first clear bit.

The clear bit defines the location of the bit in the received data. The count starts at zero. If there is no set bit this value to 255.

```
CF001 Clr Bit 1
bit: 255
```

To modify this parameter (000 to 255), use the keypad as explained in section Entering Decimal Numbers (see page 333) and press [ENTER].

A module update must be performed to each reader expander that the custom format is selected for before this can be used.

Auto-addressing

The SE firmware does not directly support Auto-addressing. The Auto-addressable modules can, however, be used with the SE system by manually assigning their addresses. This is achieved by creating a table which contains a list of module serial numbers alongside the addresses to assign.

When an Auto-addressable module is plugged in and attempts to register, the system will check it's type and serial number against this table and, if found, will assign the address that has been specified. Once the module has this address assigned it will retain the address from then on (or until deliberately changed to something else).

To access the Auto-addressing menu login in using any valid Installer code then select [MENU 4,9,6].

If there are entries already in the table then the first entry will be displayed. If the table is empty then a prompt to add an entry will be displayed.

```
ZX001
S/N 1234ABCD
```

From the prompt or from the display of the entry press [ENTER] to edit the settings or press the Up or Down arrows to select another entry. Alternately press the Left or Right arrows to see more options.

Adding and Deleting records

From the display of an auto-addressing table entry press the Left or Right arrow to scroll through the three options: *Add an entry*, *Find* and *Remove entry*. Press [ENTER] to select the option.

```
ZX001
Add an entry
```

Press [ENTER] to add an entry. A new entry will be created with default values. Press [ENTER] again to begin editing the values as described below.

```
ZX001
Remove entry
```

The current entry will be removed from the table. Note that removing an entry from the table will not affect the module itself. It simply means that the next time that module tries to register it's serial number will not be found in the table so it's address will not be checked and/or changed. If it already has a valid address then that address will be kept.

```
ZX001
Find
```

The Find function will send a command to the selected module telling it to flash it's Fault LED for 60 seconds. This can be helpful for identifying modules in a complex system. Note that the module must be online and registered for this command to be sent.

Changing Settings

When the entry is displayed as shown;

```
ZX001
S/N 1234ABCD
```

press [ENTER] to edit the settings.

```
ZX001 Type
Zone expander
```

The first setting to edit is the Type. Use the [1] and [3] keys to select the desired module type. Press[ENTER] to change the setting and proceed to the next setting.

```
ZX001 Serial Num
1234ABCD
```

The second setting to edit is the serial number. Enter the serial number using the numeric keypad. Pressing the [2] or [3] keys repeatedly will allow the entry of digits A to F of a hexadecimal value. For more information about hexadecimal data entry refer to the section Hexadecimal Data Entry (see page 335).

```
ZX001 Address
005
```

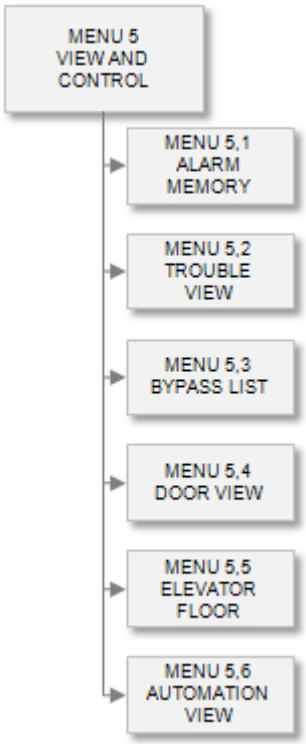
The third setting to edit is the address which is to be assigned. To enter the Address use the keypad as explained in section Entering Decimal Numbers (see page 333) then press [ENTER]. Note that this will not immediately affect the module. The address will only be checked and/or changed when the module next attempts to register with the Controller.

View

The view and control menu allows a keypad user to view the state of bypassed zones, alarm memory, current trouble conditions, control doors, control automation points and control elevator floors. To access the view and control functions, login using a valid code that is allowed view menu access and then select [MENU, 5]. Use the up and down arrows to scroll the menu items or select the menu item directly using the short cut keys.

View and Control Menu

The view and control menu consists of 6 entries that can be scrolled to using the [🡻] and [🡹] arrow or selected directly using the shortcut keys shown in the figure below.



Alarm Memory View

Alarm memory can be viewed by selecting [MENU, 5, 1] then using the [🡻] and [🡹] arrows to scroll the areas that the current user can. If an area in the list has any alarm memory associated it will be shown on the second line of the display. The [ENTER] key can be pressed to view the exact details of the alarm memory. Alarm memory is provided for each area and stores the last four different activations.

- Select the alarm memory view menu [MENU, 5, 1]. The display will show the first area that the currently logged in user has access to. This will display the alarm memory status on the second line of the display.

  ```
  Warehouse
  *Mem Empty*
  ```

- If an area does have an alarm in memory the display will show the alarm(s) in memory on the second line of the display.

  ```
  Warehouse
  *Alarms in mem*
  ```

- Pressing the [ENTER] key will display the specific zone information for the area selected this will scroll the zone information. In the following example the warehouse PIR was activated in the warehouse area.

```
Had ALARM on
Warehouse PIR
in Area
Warehouse
Press [ENTER] to
acknowledge.
Press [] to
show next item.
Press [MENU] to exit view mode.
has a battery
```

Pressing the [🡻] key will display the next zone that is stored in memory. To acknowledge memory the user must also have the acknowledge option set in their menu group or in the user configuration.

System Trouble View

System troubles can be viewed by selecting [MENU, 5, 2], trouble conditions are generated by the activation of a trouble zone. The system has 3 trouble groups (General, System and Access) with individual troubles within each group. The Protege Security System continually performs self diagnostics of system devices and monitors trouble conditions that can occur on the system. For a trouble zone to generate a trouble condition the trouble zone must belong to an area that has the 24 Hour portion of the area enabled. If a trouble condition is present in the system and trouble display option is enabled for the LCD Keypad the display will show the system trouble screen.

When a trouble condition occurs the Protege keypad can be programmed to generate an audible tone every 120 seconds. The trouble tone is cancelled when the trouble condition is viewed or the condition is returned to normal.

- Select the trouble view menu [MENU, 5, 3]. The display will show the first trouble condition if one is present and scroll a list of information.

```
*Battery*
The system or a
component of it
has a battery
problem call
service tech.
Press [ENTER] to
acknowledge.
Press [] to
show next item.
Press [MENU] to exit...
has a battery
```

The trouble view menu can also be accessed from the offline menu.

- The trouble message will scroll to show the full details of the trouble condition and action that should be taken. As shown in the example display the trouble message "The system or a component of it has a battery problem. Call service tech." is presented to the user.

Trouble Groups

Trouble groups split the available troubles in to categories that can be viewed separately. When a trouble condition occurs in a trouble group the trouble group title will be shown in place of the trouble condition in the normal trouble display.

Bypassed Zone(s) View

To view all bypassed zones in the system select **[MENU, 5, 3]**, the system will run a check and verify each zone in the system. The display will show the first zone that is bypassed and the user can then press the DOWN key to continue searching.

- Select the bypass zone view menu [**MENU, 5, 3**]. The display will show the checking zone(s) for bypass message while it is scanning all zones in the system for a bypass condition.

  ```
  Checking zone(s)
  for bypass...
  ```

- If a zone is bypassed the zone will be displayed on the screen and the prompt will ask if you wish to continue searching.

  ```
  Warehouse PIR
  Find next zone?
  ```

- Pressing the [🡻] key will display the next zone that is bypassed. Pressing the [🡹] key will begin searching from the start. If the bypass for this zone needs to be removed you can do this by selecting **[MENU, 7, 1]**, use the search feature in the zone bypass to find the zone using the text name.

  ```
  Bypass list
  completed.
  ```

If all zones have been searched the display will show the bypass list completed message above. Pressing the [🡹] key will begin searching from the start.

Viewing Door Status

Viewing the door status is identical to viewing the door status under the control menu in the advanced section. Login using a valid code and then select [**MENU, 5, 4**]. The screen displays "Select Door to view" as shown in the following example.

```
Select Door to
view: DR001
```

Type the appropriate door number or use the [🡻] and [🡹] keys to scroll the available doors. When the desired door number appears on the screen, press [**ENTER**] to view and control the selected door number.

Door Control and Status Display

Each door will display the status of the door inputs that are controlling the door and the state of the lock output that is controlled by the door configuration.

```
*Door 001
(Closed)(Locked)
```

Use the [🡻] and [🡹] keys to scroll the available doors while in the view screen, press the [**1**] key to unlock the door for the programmed unlock time, press the [**2**] key to lock the door and press the [**3**] key to activate the door latched. Press the [🡸] to return to the Door selection display.

The display will show the door input states listed below.

CLOSED	Door is closed
OPEN	Door is open
FORCED	Door is forced open
PREALM	Door is in a pre-alarm open condition
LEFTOP	Door has been left open

The display will show the door lock states listed below.

LOCKED	Lock PGM is deactivated
ACCESS	Lock PGM is activated by a user entry
SCHED	Lock PGM is activated by schedule
TIMED	Lock PGM is activated for time period by manual control
LATCH	Lock PGM is activated latched by manual control
ENTRY	Lock PGM is activated request to enter
EXIT	Lock PGM is activated request to exit
MENU	Lock PGM is activated keypad control
AREA	Lock PGM is activated by area
FIRE	Lock PGM is activated by fire control programmable function

Viewing Elevator Floor Status

Viewing the floor status is identical to viewing the floor status under the control menu in the advanced section. Login using a valid code and then select [MENU, 5, 5]. The screen displays "Elevator to view" as shown in the following example.

```
Elevator to
view: EL001
```

Type the appropriate elevator number or use the [🡻] and [🡹] keys to scroll the available elevators. When the desired elevator number appears on the screen, press [ENTER] to select the floor on the elevator to control.

Floor Selection

Once the elevator has been selected you can now select the floor to control on the elevator by using the up and down keys.

```
EL001 Floor to
view: FL001
```

Type the appropriate floor number or use the [🡻] and [🡹] keys to scroll the available floors for the selected elevator. When the desired floor number appears on the screen, press [ENTER] to view and control the selected floor number.

Floor Control and Status Display

ach floor will display the status of the floor inputs that are controlling the door and the state of the lock output that is controlled by the door configuration.

```
*Floor 001
(Locked)
```

Use the [🡻] and [🡹] keys to scroll the available floors while in the view screen, press the [1] key to unlock the floor for the programmed floor unlock time, press the [2] key to lock the floor and press the [3] key to activate the floor latched. Press the [🡸] to return to the floor selection display.

The display will show the floor relay activation states listed below.

LOCKED	Floor Relay is deactivated
SCHED	Floor Relay is activated by schedule
TIMED	Floor Relay is activated for time period by manual control or access
LATCH	Floor Relay is activated latched by manual control
AREA	Floor Relay is activated by an area

Viewing Automation Status

Viewing the automation status is identical to viewing the automation status in the offline menu when the keypad has offline automation status enabled. Login using a valid code and then select [MENU, 5, 6]. The screen displays "Automation to view" as shown in the following example.

```
Automation to
view: AT001
```

Type the appropriate automation number or use the [🡻] and [🡹] keys to scroll the available automation points that are available. When the desired automation number appears on the screen, press [ENTER] to view and control the selected automation number.

Automation Control and Status Display

Each door will display the status of the automation point.

```
*Automation 001
is OFF
```

Use the [🡻] and [🡹] keys to scroll the available automation points while in the view screen, press the [1] key to turn on the automation point for the programmed control time, press the [2] key to turn of the automation point and press the [3] key to activate the automation point latched. Press the [🡸] to return to the Automation selection display.

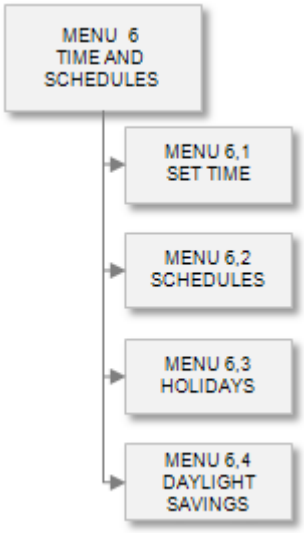
The display will show the automation states listed below.

OFF	Automation Point is deactivated
ON	Automation Point is activated by a user entry
TIMED	Automation Point is activated for time period by manual control
LATCH	Automation Point is activated latched by manual control

Time

The time menu allows a keypad user to program and configure time related settings. You are able to set the time, date and day of week, configure schedules that allow operation at certain times of the day (Scheduled Times or Time Zones), Program Holidays and configure daylight savings operation.

To access the menu, login using a valid code that is allowed time menu access and then select [MENU, 6]. Use the up and down arrows to scroll the menu items or select the menu item directly using the short cut keys.



Set Time

To access the time and date configuration, login using a valid code that has access to the time menu and then select [MENU, 6, 1]. The screen will then display the current time. Enter the time you want and then press enter, the screen will then change to the date and finally the day of the week.

It is important to accurately set the date and time and day of week for schedules and time related events to occur correctly.

To automatically adjust your time for daylight saving compensation refer to the Daylight Savings Configuration (see page 277).

Setting the System Time

The time setting uses 24 hour format. Enter the hours and minutes that you want to program the system time with, to skip over the time setting and move to the date setting press the [ENTER] key.

```
Enter system
time: 02:00
```

To modify the system time use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Setting the System Date

The date setting uses a 4 digit year and must be set with the correct century. Enter the day and month values that you want to program the system date with, to skip over the date setting and move to the day of week setting press the [ENTER] key.

```
Enter system
date: 13/07/2005
```

To modify the system date use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Setting the Day Of The Week

The system controller uses the day of the week (Monday to Sunday) to correctly perform scheduling and process time related events within the system.

```
Day of week
Monday
```

Use the [1] and [3] keys to scroll the days of the week selection and press [ENTER] to program the day of week shown. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Schedules

To access schedule programming, login using a valid code that has access to the schedule programming menu and then select [MENU, 6, 2]. The screen will then prompt you to "Select a schedule to modify" requesting that you enter a schedule number. Type the appropriate 3-digit schedule number or use the [🡻] and [🡹] keys to scroll the available schedule. When the desired schedule number appears on the screen, press [ENTER] to program the selected schedule. The maximum number of schedules that can be programmed is limited by your system's memory and configured profile.

To browse the schedules by name press [ENTER] when prompted for a schedule number to modify and then use the [🡻] and [🡹] keys to scroll the available schedules by their name.

```
Schedule to
modify: SC001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the schedule settings in the Protege System allow you to use these schedules to control operations by the time of day and day of the week.

Displaying Schedule Status

It is possible to show the current status of the schedule. This allows you to see if the schedule is active and valid, if the start time is currently valid and the end time is valid.

```
Schedule to
modify: SC001
```

Type the appropriate 3-digit schedule number or use the [🡻] and [🡹] keys. When the desired schedule appears on the screen, press the [ARM] key to display information on the selected schedule. The screen will now display status information about the schedule. Press any other key to return to the schedule selection window.

```
S: VSE
   YYn
```

The display above represents the following information for the selected schedule:

- **V** A 'Y' (yes) under the V means the schedule is valid
- **S** A 'Y' (yes) under the S means the start time of a period in the schedule is valid
- **E** A 'Y' (yes) under the S means the end time of a period in the schedule is valid

Selecting an Schedule Entry to Modify

Each schedule entry is assigned a unique schedule number from 001 to 250.

```
Schedule to
modify: SC001
```

Type the appropriate 3-digit schedule number or use the [🡻] and [🡹] keys to scroll the available schedule entries. When the desired schedule number appears on the screen, press [ENTER] to program the selected schedule entry. The maximum number of schedules that can be programmed is limited by your system's memory and configured profile.

Schedule Name

If the selected schedule entry has a name associated (some schedule entries may not have a name associated with them) the name programming screen will be shown.

```
SC001 Name
*Schedule 001
```

To scroll schedule entries by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected schedule item use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the schedule name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Schedule Miscellaneous Options

Miscellaneous options set the way the schedule will operate with the qualification PGM.

```
SC001 Misc
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Qualify Schedule if PGM is On.

- Enabled the schedule will only operate if the qualify PGM is on and will be invalidated when the PGM turns on if it was valid.
- Disabled the option will perform no action on the schedule.

Option 2 - Qualify Schedule if PGM is Off

- Enabled the schedule will only operate if the qualify PGM is OFF and will be invalidated when the PGM turns off if it was valid.
- Disabled the option will perform no action on the schedule.

Option 3, 4, 5, 6, 7 8 - Reserved

- Reserved do not modify

Qualify Schedule Using PGM

The schedule can be qualified using a PGM. This means even if the schedule is valid the schedule can be made invalid if the PGM turns on or off. This can be used to change the way a reader functions when the area arms. The qualify schedule PGM can be used to prevent access to a door if a specific output has been activated.

```
SC001 Qualify
pgm: --000:00
```

To modify the period one start time use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Period One Start Time

The schedule has a total of four periods. Each period defines a time for start and a time for end as well as the days of the week that the period is valid on. A period also has the holiday groups that define how the period functions if a holiday is active. To use period one program a starting time for the first period.

```
SC001 Start
P1 Time: --:--
```

To modify the period one start time use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Period One End Time

To use the period one program an ending time for the first period.

```
SC001 End
P1 Time: --:--
```

To modify the period one start time use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Period One Days Of Week

Program the days of the week that period one is valid on using the option entry function. Each option select value selects the appropriate day of the week.

```
SC001 P1 Days
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Monday

- Enabled the period will operate on Monday.
- Disabled the period will not operate on Monday.

Option 2 - Tuesday

- Enabled the period will operate on Tuesday.
- Disabled the period will not operate on Tuesday.

Option 3 - Wednesday

- Enabled the period will operate on Wednesday.
- Disabled the period will not operate on Wednesday.

Option 4 - Thursday

- Enabled the period will operate on Thursday.
- Disabled the period will not operate on Thursday.

Option 5 - Friday

- Enabled the period will operate on Friday.
- Disabled the period will not operate on Friday.

Option 6 - Saturday

- Enabled the period will operate on Saturday.
- Disabled the period will not operate on Saturday.

Option 7 - Sunday

- Enabled the period will operate on Sunday.
- Disabled the period will not operate on Sunday.

Option 8 - Reserved

- Reserved do not modify

Period One Holiday Group

There are eight holiday groups that can be assigned to a schedule. A holiday when active will have a holiday group(s) associated with it. If the period does not have any holiday group settings then it will not function on the day that the holiday is valid. The process is an and process, that is if any of the holiday group options are valid and any of the period holiday group settings are in common with the programmed value the schedule will operate. Each option select value selects the appropriate holiday group.

```
SC001 P1 Hols
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Holiday Group One

- Enabled the period will operate if a holiday is valid and has the group one option set.
- Disabled the period will not operate if the holiday group one is active.

Option 2 - Holiday Group Two

- Enabled the period will operate if a holiday is valid and has the group two option set.
- Disabled the period will not operate if the holiday group two is active.

Option 3 - Holiday Group Three

- Enabled the period will operate if a holiday is valid and has the group three option set.
- Disabled the period will not operate if the holiday group three is active.

Option 4 - Holiday Group Four

- Enabled the period will operate if a holiday is valid and has the group four option set.
- Disabled the period will not operate if the holiday group four is active.

Option 5 - Holiday Group Five

- Enabled the period will operate if a holiday is valid and has the group five option set.
- Disabled the period will not operate if the holiday group five is active.

Option 6 - Holiday Group Six

- Enabled the period will operate if a holiday is valid and has the group six option set.
- Disabled the period will not operate if the holiday group six is active.

Option 7 - Holiday Group Seven

- Enabled the period will operate if a holiday is valid and has the group seven option set.
- Disabled the period will not operate if the holiday group seven is active.

Option 8 - Holiday Group Eight

- Enabled the period will operate if a holiday is valid and has the group eight option set.
- Disabled the period will not operate if the holiday group eight is active.

Period Two to Period Four Configuration

Programming of period two, three and four is identical to period one.

Holidays

To access holiday programming, login using a valid code that has access to the holiday programming menu and then select [MENU, 6, 3]. The screen will then prompt you to "Select a holiday to modify" requesting that you enter a holiday number. Type the appropriate 3-digit holiday number or use the [🡻] and [🡹] keys to scroll the available holidays. When the desired holiday number appears on the screen, press [ENTER] to program the selected holiday. The maximum number of holidays that can be programmed is limited by your system's memory and configured profile.

To browse the holidays by name press [ENTER] when prompted for a holiday number to modify and then use the [🡻] and [🡹] keys to scroll the available holidays by their name.

```
Holiday to
modify: HL001
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the holiday settings in the Protege System allow you to prevent schedules from operating on a public holiday or pre-defined holidays.

Selecting Holiday to Modify

Each holiday entry is assigned a unique holiday number from 001 to 250.

```
Holiday to
modify: HL001
```

Type the appropriate 3-digit holiday number or use the [🡻] and [🡹] keys to scroll the available holiday entries. When the desired holiday number appears on the screen, press [ENTER] to program the selected holiday entry. The maximum number of holidays that can be programmed is limited by your system's memory and configured profile.

Holiday Name

If the selected holiday entry has a name associated (some holiday entries may not have a name associated with them) the name programming screen will be shown.

```
HL001 Name
*Holiday 001
```

To scroll holiday entries by name use the [🡻] and [🡹] keys. To modify or enter a new name for the selected holiday item use the keypad as explained in section Entering Text and Names (see page 333) and press [ENTER].

By default the holiday name will be prefixed by an '*' this indicates that the name is an editable name in the system.

Holiday Start Date

Program a starting date for the holiday. To make the starting date occur annually leave the year blank (----).

```
HL001 Start
Date: --/--/----
```

To modify the holiday starting date use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Holiday End Date

Program an ending date for the holiday. To make the ending date occur annually leave the year blank (----).

```
HL001 End
Date: --/--/----
```

To modify the holiday ending date use the keypad as explained in the section Entering Time and Date Values (see page 334) and press [ENTER].

Holiday Group Mask

There are eight holiday groups that can be assigned to a holiday. These form a mask used by the schedules. If a holiday is valid and a schedule has the same group set for the holiday group option then the schedule will function normally on that day.

```
HL001 Hol Mask
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1 - Holiday Group One

- Enabled the holiday will belong to group 1.
- Disabled the holiday will not belong to group 1.

Option 2 - Holiday Group Two

- Enabled the holiday will belong to group 2.
- Disabled the holiday will not belong to group 2.

Option 3 - Holiday Group Three

- Enabled the holiday will belong to group 3.
- Disabled the holiday will not belong to group 3.

Option 4 - Holiday Group Four

- Enabled the holiday will belong to group 4.
- Disabled the holiday will not belong to group 4.

Option 5 - Holiday Group Five

- Enabled the holiday will belong to group 5.
- Disabled the holiday will not belong to group 5.

Option 6 - Holiday Group Six

- Enabled the holiday will belong to group 6.
- Disabled the holiday will not belong to group 6.

Option 7 - Holiday Group Seven

- Enabled the holiday will belong to group 7.
- Disabled the holiday will not belong to group 7.

Option 8 - Holiday Group Eight

- Enabled the holiday will belong to group 8.
- Disabled the holiday will not belong to group 8.

Daylight Saving Adjustment

To access daylight saving programming, login using a valid code that has access to the daylight saving programming menu and then select [**MENU, 6, 4**]. The screen will then immediately display the daylight savings start configuration screen.

```
D/S Starts on
None
```

Every time you press the Enter key, the next screen appears. The different screens are described in the following sub-sections. Programming the daylight saving settings in the Protege System allows the system to accurately compensate for daylight savings adjustments for the time zone the system controller is located in.

Daylight Savings Start Day

The start day selects the day of the month that daylight savings will start on. Daylight savings is programmed to start on a day and end on a day for each time zone.

```
D/S Starts on
None
```

Use the [1] and [3] keys to scroll the starting day until you reach the required selection and press [ENTER] to proceed to the next daylight savings screen. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Daylight Savings Start Month

The start month selects the month that daylight savings will start in.

```
D/S Start Month
None
```

Use the [1] and [3] keys to scroll the starting month until you reach the required selection and press [ENTER] to proceed to the next daylight savings screen. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Daylight Savings End Day

The end day selects the day of the month that daylight savings will end on. Daylight savings is programmed to start on a day and end on a day for each time zone.

```
D/S Ends on
None
```

Use the [1] and [3] keys to scroll the ending day until you reach the required selection and press [ENTER] to proceed to the next daylight savings screen. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Daylight Savings End Month

The end month selects the month that daylight savings will end in.

```
D/S End Month
None
```

Use the [1] and [3] keys to scroll the ending month until you reach the required selection and press [ENTER] to proceed to the next daylight savings screen. For more information about the list control data entry refer to the section List Control Data Entry (see page 335).

Daylight Savings Options

Currently all daylight savings options are reserved.

```
D/S Options
   [--------]
```

To modify options, use the keypad as explained in section Entering Data Options (see page 336).

Option 1, 2, 3, 4, 5, 6, 7 and 8 – Reserved Do Not Modify

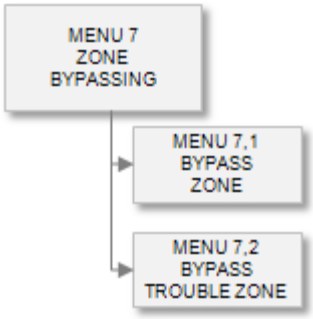
- Reserved do not modify

Bypass

To access the bypass menu, login using a valid code that is allowed bypass menu access and then select [MENU, 7]. You can then browse the bypass menu and select the bypass that you want to perform on your Protege System.

Bypass Menu

The bypass menu consists of 2 entries that can be scrolled to using the [🡻] and [🡹] arrow or selected directly using the shortcut keys shown in the figure below.



Bypassing Zones

To bypass zones select [MENU, 7, 1] then using the [🡻] and [🡹] arrows to scroll the available zones. A zone can be bypassed by pressing the [1] key to bypass the zone and then the [2] key to remove the zone bypass. A zone can also be bypassed in latch mode by pressing the [3] key. If a zone is bypassed normally [1] the zone bypass will be removed the next time the area disarms, please not all areas that have this zone programmed must disarm for the bypass to be removed.

- Select the bypass zone menu [MENU, 7, 1]. The display will show the first zone in the system.

  ```
  Warehouse PIR
  is not BYPASSED
  ```

- If a normal bypass is required press the [1] key the zone will then toggle state and the display will show the bypassed message below.

  ```
  Warehouse PIR
  is BYPASSED
  ```

- Pressing the [2] key will remove the bypass and pressing the [3] key will bypass the zone in a latched state requiring that the bypass is removed manually before it will operate again.

The Protege System also allows you to search for a zone based on the zone text that is programmed. To use the search functionality press the [MEMORY] key.

Bypassing Trouble Zones

To bypass trouble zones select [MENU, 7, 2] then using the [🡻] and [🡹] arrows to scroll the available trouble zones. A trouble zone can be bypassed by pressing the [1] key to bypass the trouble zone and then the [2] key to remove the trouble zone bypass. A trouble zone can also be bypassed in latch mode by pressing the [3] key. If a trouble zone is bypassed normally [1] the trouble zone bypass will be removed the next time the area disarms, please note that all areas that have this trouble zone programmed must disarm for the bypass to be removed.

- Select the bypass trouble zone menu [MENU, 7, 2]. The display will show the first trouble zone in the system.

```
CP001:01 T-Zone
is not BYPASSED
```

- If a normal bypass is required press the **[1]** key the trouble zone will then toggle state and the display will show the bypassed message below.

```
CP001:01 T-Zone
is BYPASSED
```

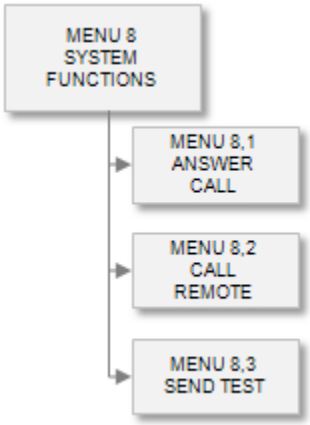
- Pressing the **[2]** key will remove the bypass and pressing the **[3]** key will bypass the trouble zone in a latched state requiring that the bypass is removed manually before it will operate again.

System

To access the event review log, login using a valid code that is allowed event menu access and then select [MENU, 3]. You can then select the event review function that you want to perform on your Protege System.

System Menu

The system menu consists of 3 entries that can be scrolled to using the [🡻] and [🡹] arrow or selected directly using the shortcut keys shown in the figure below.



Answer Incoming Call

To answer an incoming call from a remote Protege Connection select [MENU, 8, 1] then using the [🡻] and [🡹] arrows scroll the available services. Pressing the [ENTER] key will request the selected service to answer the ringing phone line.

Call Remote Host

To call a remote Protege Connection and ask it to start a connection select [MENU, 8, 2] then using the [🡻] and [🡹] arrows scroll the available services. Pressing the [ENTER] key will request the selected service to dial the programmed PC phone number for the selected service.

Send Test Zone

To activate the Test Zone select [MENU, 8, 3] then press the [ENTER] key to confirm the action. The system will then open the test zone on the system controller trouble zones. The trouble zone must be in an area that is currently armed.

Reporting Tables

Reporting tables are used to map a specific zone range to a reporting point number to allow the Protege to report the higher zone numbers used within the system over protocols that are limited in the point capacity such as Contact ID.

A reporting table is also provided for the SIA protocol to correctly display the number of a zone or trouble zone that is reported.

Contact ID Standard Zones

The following tables show the reporting codes for the zones when the Contact ID Standard Table is used (Table 000, Default). The standard table is ideally suited to small burglary and access control installations.

Control Panel Zones

The control panel will report all zones from 1 to 16 using any of the available table configurations.

Zone Number	Contact ID Code	Reporting Point Number
CP001:01	130 (Burglary)	001
CP001:02	130 (Burglary)	002
CP001:03	130 (Burglary)	003
CP001:04	130 (Burglary)	004
CP001:05	130 (Burglary)	005
CP001:06	130 (Burglary)	006
CP001:07	130 (Burglary)	007
CP001:08	130 (Burglary)	008
CP001:09	130 (Burglary)	009
CP001:10	130 (Burglary)	010
CP001:11	130 (Burglary)	011
CP001:12	130 (Burglary)	012
CP001:13	130 (Burglary)	013
CP001:14	130 (Burglary)	014
CP001:15	130 (Burglary)	015
CP001:16	130 (Burglary)	016

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported in some cases the zone number will reflect the module address that the zone was activated from to aid in service.

Keypad Zones

The keypad will report zones from 1 to 4 on the first 6 modules, all modules above address KP006 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
KP001:01	130 (Burglary)	017
KP001:02	130 (Burglary)	018
KP001:03	130 (Burglary)	019
KP001:04	130 (Burglary)	020
KP002:01	130 (Burglary)	021
KP002:02	130 (Burglary)	022
| | |	| | |	| |
KP006:04	130 (Burglary)	040
KP007:01	130 (Burglary)	999
| | |	| | |	| |
KP250:04	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report zones from 1 to 16 on the first 4 modules, all modules above address ZX004 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
ZX001:01	130 (Burglary)	041
ZX001:02	130 (Burglary)	042
ZX001:03	130 (Burglary)	043
ZX001:04	130 (Burglary)	044
ZX001:05	130 (Burglary)	045
ZX001:06	130 (Burglary)	046
ZX001:07	130 (Burglary)	047
ZX001:08	130 (Burglary)	048
ZX001:09	130 (Burglary)	049
ZX001:10	130 (Burglary)	050
ZX001:11	130 (Burglary)	051
ZX001:12	130 (Burglary)	052
ZX001:13	130 (Burglary)	053
ZX001:14	130 (Burglary)	054
ZX001:15	130 (Burglary)	055
ZX001:16	130 (Burglary)	056

Zone Number	Contact ID Code	Reporting Point Number
ZX002:01	130 (Burglary)	057
| | |	| | |	| |
ZX004:16	130 (Burglary)	104
ZX005:01	130 (Burglary)	999
| | |	| | |	| |
ZX250:16	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

2 Reader Expander

The 2 reader expander will report zones from 1 to 8 on the first 16 modules, all modules above address RD016 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
RD001:01	130 (Burglary)	105
RD001:02	130 (Burglary)	106
RD001:03	130 (Burglary)	107
RD001:04	130 (Burglary)	108
RD001:05	130 (Burglary)	109
RD001:06	130 (Burglary)	110
RD001:07	130 (Burglary)	111
RD001:08	130 (Burglary)	112
RD002:01	130 (Burglary)	113
| | |	| | |	| |
RD016:08	130 (Burglary)	232
RD017:01	130 (Burglary)	999
| | |	| | |	| |
RD250:08	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 PGM Output Expander

The 16 PGM Output expander will not report any zones as no physical connection is provided on the 16 PGM output expander. Trouble zones will be reported.

Analog Input/Output Expander

The Analog Input and Output Expanders will not report any zones as no physical connection is provided on the Analog Input and Output expanders. Trouble zones will be reported.

Contact ID Standard Trouble Zones

The following tables show the reporting codes for the trouble zones when the Contact ID Standard Table is used (Table 000, Default).

Control Panel Trouble Zones

The control panel will report all trouble zones from 1 to 64 using any of the available table configurations.

Zone Number	Contact ID Code	Reporting Point Number
CP001:01	145 (Module Tamper)	501
CP001:02	301 (AC Loss)	502
CP001:03	302 (Low System Battery)	503
CP001:04	626 (RTC Inaccurate)	504
CP001:05	602 (Periodic Test Report)	505
CP001:06	354 (Fail To Communicate)	506
CP001:07	351 (Phone Line TLM Fail)	507
CP001:08	312 (Auxiliary Fuse)	508
CP001:09	145 (Bell/Siren 1 Tamper)	509
CP001:10	145 (Bell/Siren 2 Tamper)	510
CP001:11	321 (Bell/Siren 1 Over Current)	511
CP001:12	322 (Bell/Siren 2 Over Current)	512
CP001:13	143 (Module Lost)	513
CP001:14	143 (Module Security)	514
CP001:15	330 (Expansion Card Problem)	515
CP001:16	330 (COM Port 1 Problem)	516
CP001:17	330 (COM Port 2 Problem)	517
CP001:18	330 (COM Port 3 Problem)	518
CP001:19	330 (COM Port 4 Problem)	519
CP001:20	330 (Ethernet Link Failure)	520
CP001:21	331 (DVAC Failure To Poll)	521
CP001:22	331 (ModBUS Failure To Poll)	522
CP001:23	416 (Remote Interface Login)	523
CP001:24	466 (Installer Login UN00002)	524
CP001:25	415 (Service 1 Stopped)	525
CP001:26	415 (Service 2 Stopped)	526
CP001:27	415 (Service 3 Stopped)	527
CP001:28	415 (Service 4 Stopped)	528
CP001:29	140 (General Alarm)	529
| | |	| | | | | |	| |
CP001:64	140 (General Alarm)	564

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported in some cases the zone number will reflect the module address that the zone was activated from to aid in service.

Keypad Zones

The keypad will report trouble zones from 1 to 8 on the first 6 modules, all modules above address KP006 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
KP001:01	145 (Module Tamper)	565
KP001:02	302 (Low Voltage)	566
KP001:03	120 (Panic 1+3)	567
KP001:04	121 (Duress Code)	568
KP001:05	423 (Forced Access)	569
KP001:06	426 (Door Open)	570
KP001:07	461 (Invalid Code Lockout)	571
KP001:08	143 (Module Offline)	572
KP002:01	145 (Module Tamper)	573
KP002:02	302 (Low Voltage)	574
| | |	| | |	| |
KP006:08	143 (Module Offline)	612
KP007:01	145 (Module Tamper)	999
| | |	| | |	| |
KP250:04	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report trouble zones from 1 to 16 on the first 4 modules, all modules above address ZX004 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
ZX001:01	145 (Module Tamper)	613
ZX001:02	301 (AC Loss)	614
ZX001:03	302 (Low System Battery)	615
ZX001:04	312 (Auxiliary Fuse)	616
ZX001:05	321 (Siren/Bell 1 Tamper)	617
ZX001:06	322 (Siren/Bell 2 Tamper)	618
ZX001:07	312 (Siren/Bell 1 Over Current)	619
ZX001:08	312 (Siren/Bell 2 Over Current)	620
ZX001:09	140 (General Alarm)	621

Zone Number	Contact ID Code	Reporting Point Number
ZX001:10	140 (General Alarm)	622
ZX001:11	140 (General Alarm)	623
ZX001:12	140 (General Alarm)	624
ZX001:13	140 (General Alarm)	625
ZX001:14	140 (General Alarm)	626
ZX001:15	140 (General Alarm)	627
ZX001:16	143 (Module Offline)	628
ZX002:01	145 (Module Tamper)	629
| | |	| | |	| |
ZX004:16	143 (Module Offline)	676
ZX005:01	145 (Module Tamper)	999
| | |	| | |	| |
ZX250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

2 Reader Expander

The 2 reader expander will report trouble zones from 1 to 16 on the first 16 modules, all modules above address RD016 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
RD001:01	145 (Module Tamper)	677
RD001:02	301 (AC Loss)	678
RD001:03	302 (Low System Battery)	679
RD001:04	312 (Auxiliary Fuse)	680
RD001:05	312 (Lock Trouble)	681
RD001:06	423 (Door 1 Forced)	682
RD001:07	423 (Door 2 Forced)	683
RD001:08	426 (Door 1 Left Open)	684
RD001:09	426 (Door 2 Left Open)	685
RD001:10	312 (Reader 1 Power Supply)	686
RD001:11	312 (Reader 2 Power Supply)	687
RD001:12	145 (Reader 1 Tamper)	688
RD001:13	145 (Reader 2 Tamper)	689
RD001:14	461 (Door 1 Access Attempts)	690
RD001:15	461 (Door 2 Access Attempts)	691
RD001:16	143 (Module Offline)	692
RD002:01	145 (Module Tamper)	693

Zone Number	Contact ID Code	Reporting Point Number
| | |	| | |	| |
RD016:16	143 (Module Offline)	932
RD017:01	145 (Module Tamper)	999
| | |	| | |	| |
RD250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

16 PGM Output Expander

The 16 PGM output expander will report trouble zones from 1 to 8 on the first 4 modules, all modules above address PX004 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
PX001:01	145 (Module Tamper)	933
PX001:02	301 (AC Loss)	934
PX001:03	302 (Low System Battery)	935
PX001:04	312 (Auxiliary Fuse)	936
PX001:05	312 (Relay Supply off / Fire Input off)	937
PX001:06	140 (General Alarm)	938
PX001:07	140 (General Alarm)	939
PX001:08	143 (Module Offline)	940
PX002:01	145 (Module Tamper)	941
| | |	| | |	| |
PX004:08	143 (Module Offline)	964
PX005:01	145 (Module Tamper)	999
| | |	| | |	| |
PX250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

Analog Input/Output Expander

The Analog expander will report trouble zones from 1 to 8 on the first 2 modules, all modules above address AE002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
AE001:01	145 (Module Tamper)	965
AE001:02	312 (Analog Voltage Low)	966
AE001:03	312 (Auxiliary Fuse)	967
AE001:04	140 (General Alarm)	968

Zone Number	Contact ID Code	Reporting Point Number
AE001:05	140 (General Alarm)	969
AE001:06	140 (General Alarm)	970
AE001:07	140 (General Alarm)	971
AE001:08	143 (Module Offline)	972
AE002:01	145 (Module Tamper)	973
| | |	| | |	| |
AE002:08	143 (Module Offline)	980
AE003:01	145 (Module Tamper)	999
| | |	| | |	| |
AE250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

Contact ID Large Zones

The following tables show the reporting codes for the zones when the Contact ID Large Table is used (Table 001). The large table is ideally suited to predominantly burglary based installations that are comprised of a large number of zone expansion modules.

Control Panel Zones

The control panel will report all zones from 1 to 16 using any of the available table configurations.

Zone Number	Contact ID Code	Reporting Point Number
CP001:01	130 (Burglary)	001
CP001:02	130 (Burglary)	002
CP001:03	130 (Burglary)	003
CP001:04	130 (Burglary)	004
CP001:05	130 (Burglary)	005
CP001:06	130 (Burglary)	006
CP001:07	130 (Burglary)	007
CP001:08	130 (Burglary)	008
CP001:09	130 (Burglary)	009
CP001:10	130 (Burglary)	010
CP001:11	130 (Burglary)	011
CP001:12	130 (Burglary)	012
CP001:13	130 (Burglary)	013
CP001:14	130 (Burglary)	014
CP001:15	130 (Burglary)	015
CP001:16	130 (Burglary)	016

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported in some cases the zone number will reflect the module address that the zone was activated from to aid in service.

Keypad Zones

The keypad will report zones from 1 to 4 on the first 2 modules, all modules above address KP002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
KP001:01	130 (Burglary)	017
KP001:02	130 (Burglary)	018
KP001:03	130 (Burglary)	019
KP001:04	130 (Burglary)	020
KP002:01	130 (Burglary)	021
KP002:02	130 (Burglary)	022
| | |	| | |	| |
KP002:04	130 (Burglary)	024
KP003:01	130 (Burglary)	999
| | |	| | |	| |
KP250:04	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report zones from 1 to 16 on the first 20 modules, all modules above address ZX020 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
ZX001:01	130 (Burglary)	025
ZX001:02	130 (Burglary)	026
ZX001:03	130 (Burglary)	027
ZX001:04	130 (Burglary)	028
ZX001:05	130 (Burglary)	029
ZX001:06	130 (Burglary)	030
ZX001:07	130 (Burglary)	031
ZX001:08	130 (Burglary)	032
ZX001:09	130 (Burglary)	033
ZX001:10	130 (Burglary)	034
ZX001:11	130 (Burglary)	035
ZX001:12	130 (Burglary)	036
ZX001:13	130 (Burglary)	037

Zone Number	Contact ID Code	Reporting Point Number
ZX001:14	130 (Burglary)	038
ZX001:15	130 (Burglary)	039
ZX001:16	130 (Burglary)	040
ZX002:01	130 (Burglary)	041
| | |	| | |	| |
ZX020:16	130 (Burglary)	344
ZX021:01	130 (Burglary)	999
| | |	| | |	| |
ZX250:16	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

2 Reader Expander

The 2 reader expander will report zones from 1 to 8 on the first 2 modules, all modules above address RD002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
RD001:01	130 (Burglary)	345
RD001:02	130 (Burglary)	346
RD001:03	130 (Burglary)	347
RD001:04	130 (Burglary)	348
RD001:05	130 (Burglary)	349
RD001:06	130 (Burglary)	350
RD001:07	130 (Burglary)	351
RD001:08	130 (Burglary)	352
RD002:01	130 (Burglary)	353
| | |	| | |	| |
RD002:08	130 (Burglary)	360
RD003:01	130 (Burglary)	999
| | |	| | |	| |
RD250:08	130 (Burglary)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 PGM Output Expander

The 16 PGM Output expander will not report any zones as no physical connection is provided on the 16 PGM output expander. Trouble zones will be reported.

Analog Input/Output Expander

The Analog Input and Output Expanders will not report any zones as no physical connection is provided on the Analog Input and Output expanders. Trouble zones will be reported.

Contact ID Large Trouble Zones

The following tables show the reporting codes for the trouble zones when the Contact ID Large Table is used (Table 001).

Control Panel Trouble Zones

The control panel will report all trouble zones from 1 to 64 using any of the available table configurations.

Zone Number	Contact ID Code	Reporting Point Number
CP001:01	145 (Module Tamper)	501
CP001:02	301 (AC Loss)	502
CP001:03	302 (Low System Battery)	503
CP001:04	626 (RTC Inaccurate)	504
CP001:05	602 (Periodic Test Report)	505
CP001:06	354 (Fail To Communicate)	506
CP001:07	351 (Phone Line TLM Fail)	507
CP001:08	312 (Auxiliary Fuse)	508
CP001:09	145 (Bell/Siren 1 Tamper)	509
CP001:10	145 (Bell/Siren 2 Tamper)	510
CP001:11	321 (Bell/Siren 1 Over Current)	511
CP001:12	322 (Bell/Siren 2 Over Current)	512
CP001:13	143 (Module Lost)	513
CP001:14	143 (Module Security)	514
CP001:15	330 (Expansion Card Problem)	515
CP001:16	330 (COM Port 1 Problem)	516
CP001:17	330 (COM Port 2 Problem)	517
CP001:18	330 (COM Port 3 Problem)	518
CP001:19	330 (COM Port 4 Problem)	519
CP001:20	330 (Ethernet Link Failure)	520
CP001:21	331 (DVAC Failure To Poll)	521
CP001:22	331 (ModBUS Failure To Poll)	522
CP001:23	416 (Remote Interface Login)	523
CP001:24	466 (Installer Login UN00002)	524
CP001:25	415 (Service 1 Stopped)	525
CP001:26	415 (Service 2 Stopped)	526
CP001:27	415 (Service 3 Stopped)	527

Zone Number	Contact ID Code	Reporting Point Number
CP001:28	415 (Service 4 Stopped)	528
CP001:29	140 (General Alarm)	529
| | |	| | | | | |	| |
CP001:64	140 (General Alarm)	564

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported in some cases the zone number will reflect the module address that the zone was activated from to aid in service.

Keypad Zones

The keypad will report trouble zones from 1 to 8 on the first 2 modules, all modules above address KP002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
KP001:01	145 (Module Tamper)	565
KP001:02	302 (Low Voltage)	566
KP001:03	120 (Panic 1+3)	567
KP001:04	121 (Duress Code)	568
KP001:05	423 (Forced Access)	569
KP001:06	426 (Door Open)	570
KP001:07	461 (Invalid Code Lockout)	571
KP001:08	143 (Module Offline)	572
KP002:01	145 (Module Tamper)	573
KP002:02	302 (Low Voltage)	574
| | |	| | |	| |
KP002:08	143 (Module Offline)	580
KP003:01	145 (Module Tamper)	999
| | |	| | |	| |
KP250:04	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report trouble zones from 1 to 16 on the first 20 modules, all modules above address ZX020 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
ZX001:01	145 (Module Tamper)	581
ZX001:02	301 (AC Loss)	582
ZX001:03	302 (Low System Battery)	583
ZX001:04	312 (Auxiliary Fuse)	584

Zone Number	Contact ID Code	Reporting Point Number
ZX001:05	321 (Siren/Bell 1 Tamper)	585
ZX001:06	322 (Siren/Bell 2 Tamper)	586
ZX001:07	312 (Siren/Bell 1 Over Current)	587
ZX001:08	312 (Siren/Bell 2 Over Current)	588
ZX001:09	140 (General Alarm)	589
ZX001:10	140 (General Alarm)	590
ZX001:11	140 (General Alarm)	591
ZX001:12	140 (General Alarm)	592
ZX001:13	140 (General Alarm)	593
ZX001:14	140 (General Alarm)	594
ZX001:15	140 (General Alarm)	595
ZX001:16	143 (Module Offline)	596
ZX002:01	145 (Module Tamper)	597
| | |	| | |	| |
ZX020:16	143 (Module Offline)	900
ZX021:01	145 (Module Tamper)	999
| | |	| | |	| |
ZX250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

2 Reader Expander

The 2 reader expander will report trouble zones from 1 to 16 on the first 2 modules, all modules above address RD002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
RD001:01	145 (Module Tamper)	901
RD001:02	301 (AC Loss)	902
RD001:03	302 (Low System Battery)	903
RD001:04	312 (Auxiliary Fuse)	904
RD001:05	312 (Lock Trouble)	905
RD001:06	423 (Door 1 Forced)	906
RD001:07	423 (Door 2 Forced)	907
RD001:08	426 (Door 1 Left Open)	908
RD001:09	426 (Door 2 Left Open)	909
RD001:10	312 (Reader 1 Power Supply)	910
RD001:11	312 (Reader 2 Power Supply)	911
RD001:12	145 (Reader 1 Tamper)	912

Zone Number	Contact ID Code	Reporting Point Number
RD001:13	145 (Reader 2 Tamper)	913
RD001:14	461 (Door 1 Access Attempts)	914
RD001:15	461 (Door 2 Access Attempts)	915
RD001:16	143 (Module Offline)	916
RD002:01	145 (Module Tamper)	917
| | |	| | |	| |
RD002:16	143 (Module Offline)	932
RD003:01	145 (Module Tamper)	999
| | |	| | |	| |
RD250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

16 PGM Output Expander

The 16 PGM output expander will report trouble zones from 1 to 8 on the first 2 modules, all modules above address PX002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
PX001:01	145 (Module Tamper)	933
PX001:02	301 (AC Loss)	934
PX001:03	302 (Low System Battery)	935
PX001:04	312 (Auxiliary Fuse)	936
PX001:05	312 (Relay Supply off / Fire Input off)	937
PX001:06	140 (General Alarm)	938
PX001:07	140 (General Alarm)	939
PX001:08	143 (Module Offline)	940
PX002:01	145 (Module Tamper)	941
| | |	| | |	| |
PX002:08	143 (Module Offline)	948
PX003:01	145 (Module Tamper)	999
| | |	| | |	| |
PX250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

Analog Input/Output Expander

The Analog expander will report trouble zones from 1 to 8 on the first 2 modules, all modules above address AE002 will be reported using the default code of 999.

Zone Number	Contact ID Code	Reporting Point Number
AE001:01	145 (Module Tamper)	949
AE001:02	312 (Analog Voltage Low)	950
AE001:03	312 (Auxiliary Fuse)	951
AE001:04	140 (General Alarm)	952
AE001:05	140 (General Alarm)	953
AE001:06	140 (General Alarm)	954
AE001:07	140 (General Alarm)	955
AE001:08	143 (Module Offline)	956
AE002:01	145 (Module Tamper)	957
| | |	| | |	| |
AE002:08	143 (Module Offline)	964
AE003:01	145 (Module Tamper)	999
| | |	| | |	| |
AE250:16	143 (Module Offline)	999

In the above table a reporting code of 999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

SIA Level 2 Standard Zones

The following tables show the reporting codes for the zones when the SIA Level 2 reporting format is used (Table 000, Default). The standard table is suited to both access control and burglary installations as it allows the reporting of all points available in the system.

Control Panel Zones

The control panel will report all zones from 1 to 16 using any of the available table configurations.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:01	BA	BR	0001
CP001:02	BA	BR	0002
CP001:03	BA	BR	0003
CP001:04	BA	BR	0004
CP001:05	BA	BR	0005
CP001:06	BA	BR	0006
CP001:07	BA	BR	0007
CP001:08	BA	BR	0008
CP001:09	BA	BR	0009

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:10	BA	BR	0010
CP001:11	BA	BR	0011
CP001:12	BA	BR	0012
CP001:13	BA	BR	0013
CP001:14	BA	BR	0014
CP001:15	BA	BR	0015
CP001:16	BA	BR	0016

Keypad Zones

The keypad will report zones from 1 to 4 on the first 128 modules, all modules above address KP128 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
KP001:01	BA	BR	0017
KP001:02	BA	BR	0018
KP001:03	BA	BR	0019
KP001:04	BA	BR	0020
KP002:01	BA	BR	0021
| | |	|	|	| |
KP128:04	BA	BR	0528
KP129:01	BA	BR	9999
| | |	|	|	| |
KP250:04	BA	BR	9999

In the above table a reporting code of 9999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report zones from 1 to 16 on the first 32 modules, all modules above address ZX032 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:01	BA	BR	0529
ZX001:02	BA	BR	0530
ZX001:03	BA	BR	0531
ZX001:04	BA	BR	0532
ZX001:05	BA	BR	0533
ZX001:06	BA	BR	0534
ZX001:07	BA	BR	0535
ZX001:08	BA	BR	0536

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:09	BA	BR	0537
ZX001:10	BA	BR	0538
ZX001:11	BA	BR	0539
ZX001:12	BA	BR	0540
ZX001:13	BA	BR	0541
ZX001:14	BA	BR	0542
ZX001:15	BA	BR	0543
ZX001:16	BA	BR	0544
ZX002:01	BA	BR	0545
| | |	|	|	| |
ZX032:16	BA	BR	1040
ZX033:01	BA	BR	9999
| | |	|	|	| |
ZX250:16	BA	BR	9999

2 Reader Expander

The 2 reader expander will report zones from 1 to 8 on the first 64 modules, all modules above address RD064 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
RD001:01	BA	BR	1041
RD001:02	BA	BR	1042
RD001:03	BA	BR	1043
RD001:04	BA	BR	1044
RD001:05	BA	BR	1045
RD001:06	BA	BR	1046
RD001:07	BA	BR	1047
RD001:08	BA	BR	1048
RD002:01	BA	BR	1049
| | |	|	|	| |
RD064:08	BA	BR	1552
RD065:01	BA	BR	9999
| | |	|	|	| |
RD250:08	BA	BR	9999

16 PGM Output Expander

The 16 PGM Output expander will not report any zones as no physical connection is provided on the 16 PGM output expander. Trouble zones will be reported.

Analog Input/Output Expander

The Analog Input and Output Expanders will not report any zones as no physical connection is provided on the Analog Input and Output expanders. Trouble zones will be reported.

SIA Level 2 Standard Trouble Zones

The following tables show the reporting codes for the trouble zones when the SIA Level 2 Standard Table is used (Table 000, Default).

Control Panel Trouble Zones

The control panel will report all trouble zones from 1 to 64 using any of the available table configurations.

Zone Number	Alarm Code	Restore Code		Reporting Point Number
CP001:01	TA	TH	01 Tamper	5001
CP001:02	AT	AR	02 AC	5002
CP001:03	YT	YR	03 Battery	5003
CP001:04	JT	UH	04 RTC	5004
CP001:05	TX	UJ	05 Test Report	5005
CP001:06	YC	UH	06 Report Fail	5006
CP001:07	LT	LR	07 Phone Line	5007
CP001:08	YP	YQ	08 AUX Fuse	5008
CP001:09	YP	YQ	09 NET Fuse	5009
CP001:10	YA	YH	10 PGM 3 Cut	5010
CP001:11	YA	YH	11 PGM 4 Cut	5011
CP001:12	YA	YH	12 PGM 3 OC	5012
CP001:13	YA	YH	13 PGM 4 OC	5013
CP001:14	ET	ER	14 MOD Loss	5014
CP001:15	ET	ER	15 MOD Security	5015
CP001:16	UA	UH	16 Extension Missing	5016
CP001:17	UA	UH	17 LPT 1	5017
CP001:18	UA	UH	18 LPT 2	5018
CP001:19	UA	UH	19 COM 1	5019
CP001:20	UA	UH	20 COM 2	5020
CP001:21	UA	UH	21 COM 3	5021
CP001:22	UA	UH	22 COM 4	5022
CP001:23	UA	UH	23 EtherNet Failure	5023
CP001:24	UA	UH	24 DVAC Fault	5024
CP001:25	UA	UH	25 Modbus Poll Failure	5025
CP001:26	RB	RS	26 Upload Login	5026
CP001:27	LB	LX	27 Installer Login	5027

Zone Number	Alarm Code	Restore Code		Reporting Point Number
CP001:28	YC	YK	28 Service 1 Fault	5028
CP001:29	YC	YK	29 Service 2 Fault	5029
CP001:30	YC	YK	30 Service 3 Fault	5030
CP001:31	YC	YK	31 Service 4 Fault	5031
CP001:32	UA	UH		5032
| | |	|	|		| |
CP001:64	UA	UH		5064

Keypad Trouble Zones

The keypad will report trouble zones from 1 to 8 on the first 128 modules, all modules above address KP128 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code		Reporting Point Number
KP001:01	TA	TH	01 Tamper	5065
KP001:02	UA	UH	02 Power	5066
KP001:03	PA	PH	03 Panic	5067
KP001:04	HA	HH	04 Duress	5068
KP001:05	DH	DR	05 Left Open	5069
KP001:06	DF	DR	06 Forced Open	5070
KP001:07	JA	UJ	07 Locked Out	5071
KP001:08	EM	EN	08 Communication	5072
KP002:01	TA	TH	01 Tamper	5073
| | |	|	|		| |
KP128:08	EM	EN	08 Communication	6088
KP129:01	UA	UH		9999
| | |	|	|		| |
KP250:08	UA	UH		9999

In the above table a reporting code of 9999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander Trouble Zones

The 16 zone expander will report trouble zones from 1 to 16 on the first 32 modules, all modules above address ZX032 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code		Reporting Point Number
ZX001:01	TA	TH	01 Tamper	6089
ZX001:02	AT	AR	02 AC	6090

Zone Number	Alarm Code	Restore Code		Reporting Point Number
ZX001:03	YT	YR	03 Batt	6091
ZX001:04	YP	YQ	04 Aux	6092
ZX001:05	YP	YQ	05 Network	6093
ZX001:06	YA	YH	06 PGM 3 Cut	6094
ZX001:07	YA	YH	07 PGM 4 Cut	6095
ZX001:08	YA	YH	08 PGM 3 OC	6096
ZX001:09	YA	YH	09 PGM 4 OC	6097
ZX001:10	UA	UH	10 Spare	6098
ZX001:11	UA	UH	11 Spare	6099
ZX001:12	UA	UH	12 Spare	6100
ZX001:13	UA	UH	13 Spare	6101
ZX001:14	UA	UH	14 Spare	6102
ZX001:15	UA	UH	15 Spare	6103
ZX001:16	EM	EN	16 Communication	6104
ZX002:01	TA	TH	01 Tamper	6105
| | |	|	|		| |
ZX032:16	EM	EN	16 Communication	6600
ZX033:01	UA	UH		9999
| | |	|	|		| |
ZX250:16	UA	UH		9999

In the above table a reporting code of 9999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

2 Reader Expander Trouble Zones

The 2 reader expander will report trouble zones from 1 to 16 on the first 64 modules, all modules above address RD064 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code		Reporting Point Number
RD001:01	TA	TH	01 Tamper	6601
RD001:02	AT	AR	02 AC	6602
RD001:03	YT	YR	03 Batt	6603
RD001:04	YP	YQ	04 Aux	6604
RD001:05	YP	YQ	05 Network	6605
RD001:06	DF	DR	06 D1 Forced	6606
RD001:07	DF	DR	07 D2 Forced	6607
RD001:08	DM	DH	08 D1 Left Open	6608
RD001:09	DM	DH	09 D2 Left Open	6609

Zone Number	Alarm Code	Restore Code		Reporting Point Number
RD001:10	UT	UJ	10 R1 Voltage	6610
RD001:11	UT	UJ	11 R2 Voltage	6611
RD001:12	TT	TJ	12 R1 Tamper	6612
RD001:13	TT	TJ	13 R2 Tamper	6613
RD001:14	JA	UJ	14 D1 Attempts	6614
RD001:15	JA	UJ	15 D2 Attempts	6615
RD001:16	EM	EN	16 Communication	6616
RD002:01	AT	AR	02 AC	6617
| | |	|	|		| |
RD064:16	EM	EN	16 Communication	7624
RD065:01	UA	UH		9999
| | |	|	|		| |
RD250:16	UA	UH		9999

In the above table a reporting code of 9999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

16 PGM Output Expander

The 16 PGM output expander will report trouble zones from 1 to 8 on the first 16 modules, all modules above address PX016 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code		Reporting Point Number
PX001:01	TA	TH	01 Tamper	7625
PX001:02	AT	AR	02 AC	7626
PX001:03	YT	YR	03 Batt	7627
PX001:04	YP	YQ	04 Aux	7628
PX001:05	YP	YQ	05 Network	7629
PX001:06	UA	UH	06 Spare	7630
PX001:07	UA	UH	07 Spare	7631
PX001:08	EM	EN	08 Communication	7632
PX002:01	TA	TH	01 Tamper	7633
| | |	|	|		| |
PX016:08	EM	EN	08 Communication	7752
PX017:01	UA	UH		9999
| | |	|	|		| |
PX250:08	UA	UH		9999

In the above table a reporting code of 9999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

Analog Input/Output Expander Trouble Zones

The Analog Input and Output Expanders will report trouble zones from 1 to 8 on the first 32 modules, all modules above address AE032 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
AE001:01	UA	UH	9999
AE001:02	UA	UH	9999
AE001:03	UA	UH	9999
AE001:04	UA	UH	9999
AE001:05	UA	UH	9999
AE001:06	UA	UH	9999
AE001:07	UA	UH	9999
AE001:08	UA	UH	9999
AE002:01	UA	UH	9999
| | |	|	|	| |
AE032:08	UA	UH	9999
AE033:01	UA	UH	9999
| | |	|	|	| |
AE250:08	UA	UH	9999

In the above table a reporting code of 9999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

DVAC Surgard Zone

The following tables show the reporting codes for the zones when the DVAC Surgard Reporting format is used. A DVAC reporting code is the actual code that is transmitted on the DVAC communication line, this code is more than likely translated by the alarm monitoring receiving unit in to a SIA or similar reporting code. The associated code is shown in the following table in brackets to help diagnose DVAC reporting data.

The DVAC communication format is extremely limited in the capacity that it can communicate and therefore a large number of zones are group on to a maximum zone number when reported. This limitation is due to the capacity of the DVAC protocol.

Control Panel Zones

The control panel will report all zones from 1 to 16 using any of the available table configurations.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:01	09 (BA)	89 (BR)	0001
CP001:02	09 (BA)	89 (BR)	0002
CP001:03	09 (BA)	89 (BR)	0003
CP001:04	09 (BA)	89 (BR)	0004
CP001:05	09 (BA)	89 (BR)	0005
CP001:06	09 (BA)	89 (BR)	0006
CP001:07	09 (BA)	89 (BR)	0007

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:08	09 (BA)	89 (BR)	0008
CP001:09	09 (BA)	89 (BR)	0009
CP001:10	09 (BA)	89 (BR)	0010
CP001:11	09 (BA)	89 (BR)	0011
CP001:12	09 (BA)	89 (BR)	0012
CP001:13	09 (BA)	89 (BR)	0013
CP001:14	09 (BA)	89 (BR)	0014
CP001:15	09 (BA)	89 (BR)	0015
CP001:16	09 (BA)	89 (BR)	0016

Keypad Zones

The keypad will report zones from 1 to 4 on the first 6 modules, all modules above address KP006 will be reported using the default code of 0999 using the standard 09 and 89 alarm codes.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
KP001:01	09 (BA)	89 (BR)	0017
KP001:02	09 (BA)	89 (BR)	0018
KP001:03	09 (BA)	89 (BR)	0019
KP001:04	09 (BA)	89 (BR)	0020
KP002:01	09 (BA)	89 (BR)	0021
| | |	|	|	| |
KP006:04	09 (BA)	89 (BR)	0040
KP007:01	09 (BA)	89 (BR)	0999
| | |	|	|	| |
KP250:04	09 (BA)	89 (BR)	0999

In the above table a reporting code of 9999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report zones from 1 to 16 on the first 10 modules, all modules above address ZX010 will be reported using the default code of 0999 using the standard 09 and 89 reporting codes.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:01	09 (BA)	89 (BR)	0041
ZX001:02	09 (BA)	89 (BR)	0042
ZX001:03	09 (BA)	89 (BR)	0043
ZX001:04	09 (BA)	89 (BR)	0044
ZX001:05	09 (BA)	89 (BR)	0045
ZX001:06	09 (BA)	89 (BR)	0046

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:07	09 (BA)	89 (BR)	0047
ZX001:08	09 (BA)	89 (BR)	0048
ZX001:09	09 (BA)	89 (BR)	0049
ZX001:10	09 (BA)	89 (BR)	0050
ZX001:11	09 (BA)	89 (BR)	0051
ZX001:12	09 (BA)	89 (BR)	0052
ZX001:13	09 (BA)	89 (BR)	0053
ZX001:14	09 (BA)	89 (BR)	0054
ZX001:15	09 (BA)	89 (BR)	0055
ZX001:16	09 (BA)	89 (BR)	0056
ZX002:01	09 (BA)	89 (BR)	0057
| | |	|	|	| |
ZX010:16	09 (BA)	89 (BR)	0200
ZX011:01	09 (BA)	89 (BR)	0999
| | |	|	|	| |
ZX250:16	09 (BA)	89 (BR)	0999

2 Reader Expander

The 2 reader expander will report zones from 1 to 8 on the first 2 modules, all modules above address RD002 will be reported using the default code of 0999 and the standard 09 and 89 reporting codes.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
RD001:01	09 (BA)	89 (BR)	0201
RD001:02	09 (BA)	89 (BR)	0202
RD001:03	09 (BA)	89 (BR)	0203
RD001:04	09 (BA)	89 (BR)	0204
RD001:05	09 (BA)	89 (BR)	0205
RD001:06	09 (BA)	89 (BR)	0206
RD001:07	09 (BA)	89 (BR)	0207
RD001:08	09 (BA)	89 (BR)	0208
RD002:01	09 (BA)	89 (BR)	0209
| | |	|	|	| |
RD002:08	09 (BA)	89 (BR)	0216
RD003:01	09 (BA)	89 (BR)	0999
| | |	|	|	| |
RD250:08	09 (BA)	89 (BR)	9999

16 PGM Output Expander

The 16 PGM Output expander will not report any zones as no physical connection is provided on the 16 PGM output expander. Trouble zones will be reported.

DVAC Surgard Trouble Zones

The following tables show the reporting codes for the trouble zones when the DVAC reporting service is used.

Control Panel Trouble Zones

The control panel will report all trouble zones from 1 to 64 using any of the available table configurations.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:01	37 (UT)	B7 (UJ)	0501
CP001:02	3A (AT)	BA (AR)	0502
CP001:03	3D (YT)	BD (YR)	0503
CP001:04	34 (UT)	B4 (UJ)	0504
CP001:05	3E (LT)	BE (LR)	0505
CP001:06	3E (LT)	BE (LR)	0506
CP001:07	3E (LT)	BE (LR)	0507
CP001:08	34 (YP)	B4 (YQ)	0508
CP001:09	34 (YA)	B4 (YH)	0509
CP001:10	38 (YA)	B8 (YH)	0510
CP001:11	38 (YA)	B8 (YH)	0511
CP001:12	75 (US)	F5 (UJ)	0512
CP001:13	75 (US)	F5 (UJ)	0513
CP001:14	75 (US)	F5 (UJ)	0514
CP001:15	34 (UA)	B4 (UJ)	0515
CP001:16	34 (UA)	B4 (UJ)	0516
CP001:17	34 (UA)	B4 (UJ)	0517
CP001:18	34 (UA)	B4 (UJ)	0518
CP001:19	34 (UA)	B4 (UJ)	0519
CP001:20	34 (UA)	B4 (UJ)	0520
CP001:21	34 (UA)	B4 (UJ)	0521
CP001:22	34 (UA)	B4 (UJ)	0522
CP001:23	34 (UA)	B4 (UJ)	0523
CP001:24	34 (UA)	B4 (UJ)	0524
CP001:25	34 (UA)	B4 (UJ)	0525
CP001:26	34 (UA)	B4 (UJ)	0526
CP001:27	34 (UA)	B4 (UJ)	0527
CP001:28	34 (UA)	B4 (UJ)	0528

Zone Number	Alarm Code	Restore Code	Reporting Point Number
CP001:29	34 (UA)	B4 (UJ)	0529
| | |	|	|	| |
CP001:64	34 (UA)	B4 (UJ)	0564

Keypad Zones

The keypad will report trouble zones from 1 to 8 on the first 128 modules, all modules above address KP006 will be reported using the default code of 9999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
KP001:01	37 (UT)	B7 (UJ)	0565
KP001:02	3C (YP)	BC (YQ)	0566
KP001:03	22 (PT)	A2 (PJ)	0567
KP001:04	23 (HT)	A3 (HJ)	0568
KP001:05	34 (UT)	B4 (UJ)	0569
KP001:06	34 (UT)	B4 (UJ)	0570
KP001:07	34 (UT)	B4 (UJ)	0571
KP001:08	38 (UT)	B8 (UJ)	0572
KP002:01	37 (UT)	B7 (UJ)	0573
| | |	|	|	| |
KP006:08	38 (UT)	B8 (UJ)	0612
KP007:01	37 (UT)	B7 (UJ)	0999
| | |	|	|	| |
KP250:08	38 (UA)	B8 (UJ)	0999

In the above table a reporting code of 0999 indicates that the zone is outside the maximum zones that can be reported for the module type.

16 Zone Expander

The 16 zone expander will report trouble zones from 1 to 16 on the first 10 modules, all modules above address ZX010 will be reported using the default code of 0999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:01	37 (UT)	B7 (UJ)	0613
ZX001:02	3A (AT)	BA (AR)	0614
ZX001:03	3D (YT)	BD (YR)	0615
ZX001:04	3C (LT)	BC (LR)	0616
ZX001:05	34 (YP)	B4 (YQ)	0617
ZX001:06	34 (YA)	B4 (YH)	0618
ZX001:07	38 (YA)	B8 (YH)	0619
ZX001:08	38 (YA)	B8 (YH)	0620

Zone Number	Alarm Code	Restore Code	Reporting Point Number
ZX001:09	34 (UA)	B4 (UJ)	0621
ZX001:10	34 (UA)	B4 (UJ)	0622
ZX001:11	34 (UA)	B4 (UJ)	0623
ZX001:12	34 (UA)	B4 (UJ)	0624
ZX001:13	34 (UA)	B4 (UJ)	0625
ZX001:14	34 (UA)	B4 (UJ)	0626
ZX001:15	34 (UA)	B4 (UJ)	0627
ZX001:16	38 (UT)	B8 (UJ)	0628
ZX002:01	37 (UT)	B7 (UJ)	0629
| | |	|	|	| |
ZX010:16	38 (UT)	B8 (UJ)	0772
ZX011:01	37 (UT)	B7 (UJ)	0999
| | |	|	|	| |
ZX250:16	38 (UT)	B8 (UJ)	0999

In the above table a reporting code of 0999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

2 Reader Expander

The 2 reader expander will report trouble zones from 1 to 16 on the first 2 modules, all modules above address RD003 will be reported using the default code of 0999.

Zone Number	Alarm Code	Restore Code	Reporting Point Number
RD001:01	37 (UT)	B7 (UJ)	0773
RD001:02	3A (AT)	BA (AR)	0774
RD001:03	3D (YT)	BD (YR)	0775
RD001:04	3C (LT)	BC (LR)	0776
RD001:05	38 (UT)	B4 (UJ)	0777
RD001:06	34 (UA)	B4 (UJ)	0778
RD001:07	34 (UA)	B4 (UJ)	0779
RD001:08	34 (UA)	B4 (UJ)	0780
RD001:09	34 (UA)	B4 (UJ)	0781
RD001:10	34 (UA)	B4 (UJ)	0782
RD001:11	34 (UA)	B4 (UJ)	0783
RD001:12	34 (UA)	B4 (UJ)	0784
RD001:13	34 (UA)	B4 (UJ)	0785
RD001:14	34 (UA)	B4 (UJ)	0786
RD001:15	34 (UA)	B4 (UJ)	0787
RD001:16	38 (UT)	B8 (UJ)	0788

Zone Number	Alarm Code	Restore Code	Reporting Point Number
RD002:01	37 (UT)	B7 (UJ)	0789
| | |	|	|	| |
RD002:16	38 (UT)	B8 (UJ)	0804
RD003:01	37 (UT)	B7 (UJ)	0999
| | |	|	|	| |
RD250:16	38 (UT)	B8 (UJ)	0999

In the above table a reporting code of 0999 indicates that the trouble zone is outside the maximum trouble zones that can be reported for the module type.

Reporting Codes

Custom reporting codes are assigned to zone types to override the default reporting code used for a specific alarm event. The following lists detail the reporting code used for each zone and trouble zone.

In some cases a reporting code may also be transmitted as the actual numerical value that is programmed (ModBUS Remote) in which case the physical mapping will be done in the receiving system application.

ModBUS Remote allows the monitoring of large SCADA based systems using the Protege System without the need to modify a new front end. For information on the ModBUS Slave and ModBUS Remote protocols refer to Application Note *AN-023 Protege Controller ModBUS Slave Configuration and Register Map* which explains in detail the operation of the ModBUS functions.

Area Reporting Codes

Area reporting codes are used to report the opening and closing of an area (arming and disarming) to the central station receiver or monitoring station. These codes are predefined by the protocol that is being used.

Custom Reporting Codes

Custom reporting codes allow the zone type that is assigned to a zone to alter the reporting code that is being used when reporting in Contact ID or in SIA formats.

CID (Contact ID)

Contact ID is a DTMF reporting protocol that uses a 3 digit account code and 3 digit reporting codes for each alarm transmission type. It is also possible to assign a special code to the zone type being used for a specific group of zones if needed. The custom types are shown in the table following the zone types assigned to each module.

Zones are reported using the standard burglary codes.

Alarm / Open	130 (Burglary)	(R For Restore)
Tamper	137 (Burglary Tamper)	(R For Restore)
Bypass	570 (Zone Bypass)	(R For Restore)

Contact ID Message Format

The format of the Contact ID message that is sent to the Monitoring Station receiver is static and does not change from the standard specified SIA DC-05-1999.09 reorder code 14085.

The message composition is in the following form:

ACCT MT QXYZ GG CCC S

Where:

ACCT	4 Digit Account Number composed using the digits 0-9 and B-F.
MT	Message Type. This two digit sequence is used to identify the Contact ID message to the receiver. It may be transmitted as 18 (preferred) or 98 (optional). The Protege System Controller ONLY transmits the 18 identifier.
Q	Event Qualifier 1 = New Event or Opening 3 = New Restore or Closing 6 = Previously reported condition still present (Status Report)

XYZ	3 Digit Event Code composed using the digits 0-9 and B-F.
GG	Group or Partition (Area) number composed using two hex digits 0-9 and B-F. Use 00 to indicate that no specific group or partition information is applicable.
CCC	Zone Number (Event Reports) or User Number for (Open / Close Reports) composed using the digits 0-9 and B-F. Use 000 to indicate that no specific zone or user information applies.
S	Sum of all digits + S such that a MOD 15 will result in a 0. Not a 0 shall be transmitted as a 10 and valued as a 10 for checksum purposes even though it is displayed and printed as a '0'.

The Protege System controller does not change or alter messages from this format when Contact ID is selected as the reporting format.

SIA L2 (SIA Level Two)

SIA Level Two is a modem based reporting format that is ideal for large scale integrated solutions such as the Protege System. Comprising of a multiple message format and tonal acknowledgement the SIA (Security Industry Association) format provides many reporting features ideal for access control, automation and large burglary.

The SIA protocol is pre-defined and requires no further programming to operate with the exception of an account code for an area or service that is running SIA. It is also possible to assign a special code to the zone type being used for reporting if needed. The custom types are shown in the table following the zone types assigned to each module.

Zones are reported using the standard burglary codes as detailed below. Openings, closings and other area operations are reported used the area reporting codes.

Alarm / Open	BA	BR
Tamper	BT	BJ
Bypass	BB	BR

SIA Level 2 Message Format

The format of the SIA messages can vary greatly depending on the leading zero's configuration for each of the various data code packets that can be sent. Given the large number of zones, users and areas the Protege System attempts to use the maximum of these that is available. Some provision is provided to reduce the size of these fields (Account Code to 4 Digits, Zone Numbers to 4 Digits) to allow easy integration with monitoring software.

When configuring the automation software at the monitoring station for the information coming from the receiver the following format should be used. In most cases a 4 digit account code can be set in the service and used as default.

The first transmitted data is always the account code block, this is not shown and typically prefixed with a D or F dependent on the size of the account code. This can be either 4 or 6 digits (D# or F#).

N ri GGG BA WXYZ ....

Where:

N	Signifies a new event or an O will signify a old event that is being reported.
ri GGG	The area or partition that is being reported from 000 to 999.
BA	Event Code In the example the event code is BA (Burglary Alarm) however there are a large number of event codes, refer to the reporting maps for more information.
WXYZ	4 Digit zone or user number that generate the event code.

There are various options that can be selected to change the method in which the system will report the message. The size of the account code, zones and user numbers can be changed to allow more flexible configurations however it is not recommended to change from the standard configuration.

DVAC (Surgard)

The DVAC reporting format is a hard line communication format used in North America over the Bell Telecom network. Normal burglar and zone reporting events use the standard zone reporting codes for alarm, restore, tamper and bypass. Special codes can be assigned to a zone type when reporting if variations to the codes are required, for an example a refrigeration alarm can be sent using a special code of 27.

Zones are reported using the standard DVAC burglary codes.

Alarm / Open	09 (BA) Burglary Alarm	89 (BR) Burglary Restore
Tamper	29 (TA) Burglary Tamper	A9 (TH) Tamper Restore
Bypass	49 (ZB) Zone Bypass	C9 (ZH) Bypass Removed

ModBUS Remote

ModBUS Remote is a highly flexible modem based reporting format that is ideal for large scale integrated SCADA solutions that connect to a third party ModBUS remote receiver. (It is recommended to use a Protege System Controller in remote ModBUS receive mode).

With the ability to activate specific registers and transfer data according to preset values the ModBUS remote reporting function is ideal for monitoring wide spread buildings, utility systems, city property and state wide facilities.

The ModBUS remote service works on the use of the account code as an offset to the specific point number that must be activated in the remote monitoring system which is usually connected to display graphic on a SCADA control system such as Citect, WonderWare, The FIX or DAQ Factory.

By setting an account code for the service and the reporting type in the zone type configuration the desired point will be activated at the central receiving location that is operating a Protege Controller in ModBUS receiver mode.

Trouble Zone Maps

Following is a list of all the trouble zones assigned to each of the Protege System modules. Trouble zones are used to monitor the status of the Protege System and are linked to communication failures, power supply conditions and enclosure tamper inputs.

In many cases the actual trouble zone is not physically connected to an external device, for example a module communication failure trouble zone will open when a module fails to send a poll event to the Protege System controller, the trouble zone will restore when the module returns back online.

Trouble zones are a very powerful programming tool within the Protege System that gives you absolute control over your system and how the monitoring and presentation of system trouble conditions function.

Control Panel

The following lists the trouble zones that operate on the control panel. The control panel has 64 trouble zones. Trouble zones that are reserved should not be included in an area.

Zone Number	Description	Type	Group
CP001:01	Module Tamper	System Tamper	System
CP001:02	AC failure	Power Fault	General
CP001:03	Low Battery	Power Fault	General
CP001:04	Real Time Clock Not Set	RTC/Clock Loss	General
CP001:05	Service Report Test	*	*
CP001:06	Service Report Failure To Communicate	Reporting Failure	General
CP001:07	Phone Line Fault	Phone Line Lost	General
CP001:08	Auxiliary Failure	Power Fault	General
CP001:09	Bell 1 Cut/Tamper	Bell/PGM Fault	General
CP001:10	Bell 2 Cut/Tamper	Bell/PGM Fault	General
CP001:11	Bell 1 Over Current	Bell/PGM Fault	General
CP001:12	Bell 2 Over Current	Bell/PGM Fault	General
CP001:13	Module Communication	Module Loss	System
CP001:14	Module Network Security	Module Security	System
CP001:15	Expansion Device Missing	Hardware Fault	System
CP001:16	Communication Port 1 Fault	Hardware Fault	System
CP001:17	Communication Port 2 Fault	Hardware Fault	System
CP001:18	Communication Port 3 Fault	Hardware Fault	System
CP001:19	Communication Port 4 Fault	Hardware Fault	System
CP001:20	Ethernet Link Lost	Hardware Fault	System
CP001:21	DVAC Line Fault/Polling Error	Hardware Fault	System
CP001:22	ModBUS Communication Fault	Hardware Fault	System
CP001:23	Protege Access	Hardware Fault	System
CP001:24	Installer Logged In	Hardware Fault	System

Zone Number	Description	Type	Group
CP001:25	Service 1 Stopped	Hardware Fault	System
CP001:26	Service 2 Stopped	Hardware Fault	System
CP001:27	Service 3 Stopped	Hardware Fault	System
CP001:28	Service 4 Stopped	Hardware Fault	System
CP001:29	Reserved	*	*
| || |	| |	|	|
CP001:64	Reserved	*	*

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. This can be done if required but is not recommended.

LCD Keypad

The following lists the trouble zones that operate on the LCD keypad module. The LCD keypad module has 8 trouble zones.

Zone Number	Description	Type	Group
KPxxx:01	Module Tamper	System Tamper	System
KPxxx:02	Power Trouble	Power Fault	General
KPxxx:03	Panic	*	*
KPxxx:04	Duress	*	*
KPxxx:05	Door Left Open	Left Open	Access
KPxxx:06	Door Forced Open	Forced Door	Access
KPxxx:07	Invalid Code Lockout	Attempts	Access
KPxxx:08	Module Offline	Module Offline	System

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. This can be done if required but is not recommended.

When using the reference table the LCD keypad address should be used in place of the 'xxx'.

Zone Expander

The following lists the trouble zones that operate on the zone expander module. The zone expander module has 8 trouble zones.

Zone Number	Description	Type	Group
ZXxxx:01	Module Tamper	System Tamper	System
ZXxxx:02	AC failure	Power Fault	General
ZXxxx:03	Low Battery	Power Fault	General
ZXxxx:04	Aux Failure	Power Fault	General
ZXxxx:05	Bell 1 Cut/Tamper	Bell/PGM Fault	General
ZXxxx:06	Bell 2 Cut/Tamper	Bell/PGM Fault	General
ZXxxx:07	Bell 1 Over Current	Bell/PGM Fault	General

Zone Number	Description	Type	Group
ZXxxx:08	Bell 2 Over Current	Bell/PGM Fault	General
ZXxxx:09	Reserved	*	*
ZXxxx:10	Reserved	*	*
ZXxxx:11	Reserved	*	*
ZXxxx:12	Reserved	*	*
ZXxxx:13	Reserved	*	*
ZXxxx:14	Reserved	*	*
ZXxxx:15	Reserved	*	*
ZXxxx:16	Module Offline	Module Offline	System

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. A trouble group and type can be assigned if required but is not recommended for reserved zones.

When using the reference table the zone expander address should be used in place of the 'xxx'.

PGM Expander

The following lists the trouble zones that operate on the PGM expander module. The PGM expander module has 8 trouble zones.

Zone Number	Description	Type	Group
PGxxx:01	Module Tamper	System Tamper	System
PGxxx:02	AC failure	Power Fault	General
PGxxx:03	Low Battery	Power Fault	General
PGxxx:04	Aux Failure	Power Fault	General
PGxxx:05	Relay Supply Failure	Power Fault	General
PGxxx:06	Reserved	*	*
PGxxx:07	Reserved	*	*
PGxxx:08	Module Offline	Module Offline	System

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. This can be done if required but is not recommended.

When using the reference table the PGM expander address should be used in place of the 'xxx'.

Reader Expander

The following lists the trouble zones that operate on the reader expander module. The reader expander module has 16 trouble zones.

Zone Number	Description	Type	Group
RDxxx:01	Module Tamper	System Tamper	System
RDxxx:02	AC failure	Power Fault	General
RDxxx:03	Low Battery	Power Fault	General
RDxxx:04	Aux Failure	Power Fault	General

Zone Number	Description	Type	Group
RDxxx:05	Lock Failure	Power Fault	General
RDxxx:06	Door 1 Forced	Forced Door	Access
RDxxx:07	Door 2 Forced	Forced Door	Access
RDxxx:08	Door 1 Left Open	Left Open	Access
RDxxx:09	Door 2 Left Open	Left Open	Access
RDxxx:10	Reader 1 Voltage	Power Fault	General
RDxxx:11	Reader 2 Voltage	Power Fault	General
RDxxx:12	Reader 1 Tamper	System Tamper	System
RDxxx:13	Reader 2 Tamper	System Tamper	System
RDxxx:14	Door 1 Lockout	Attempts	Access
RDxxx:15	Door 2 Lockout	Attempts	Access
RDxxx:16	Module Offline	Module Offline	System

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. This can be done if required but is not recommended.

When using the reference table the reader expander address should be used in place of the 'xxx'.

Analog Expander

The following lists the trouble zones that operate on the Analog expander module. The Analog expander module has 8 trouble zones.

Zone Number	Description	Type	Group
AExxx:01	Module Tamper	System Tamper	System
AExxx:02	Analog Power	Power Fault	General
AExxx:03	Aux Power	Power Fault	General
AExxx:04	Reserved	*	*
AExxx:05	Reserved	*	*
AExxx:06	Reserved	*	*
AExxx:07	Reserved	*	*
AExxx:08	Module Offline	Module Offline	System

In the above table a '*' indicates that the trouble zone will not generate a system trouble as by default it is not assigned a trouble type or group. This can be done if required but is not recommended.

When using the reference table the analog expander address should be used in place of the 'xxx'.

Profiles

Profiles are used to divide up the available memory in to regions that can be used for specific applications. For example an access control configuration may require more users than a burglary configuration and this is how the various profiles are designed. There are seven profiles that are predefined and one that can be configured manually.

By default manual configuration is disabled. To manually configure a profile please contact Integrated Control Technology or logon to the ICT website (http://www.incontrol.co.nz) for more information.

Standard Profile

The standard profile is the default protocol and covers the majority of all installation requirements. A good number of users and doors allows many combinations of burglary and access control to be achieved.

Description	Number
LCD Keypad Modules (PRT-KLCD)	32
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	16
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	8
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	8
Zone Inputs	464
Trouble Zone Inputs	704
PGM Outputs	420
PGM Groups	128
Area Groups	32
Menu Groups	16
Door Groups	128
Keypad Groups	32
Areas	32
Access Levels	128
Zone Types	128
Doors	16
Door Types	8
Services	8
Phone Numbers	16
Schedules	128
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	32
Panel Configuration Information	1
Users	2000
Events	2000

Description	Number
User Names	2000
Area Names	32
Access Level Names	128
Zone Type Names	64
Zone Input Names	752
Home Names	16
Door Names	16
Door Type Names	8
Area Group Names	64
Menu Group Names	16
Keypad Group Names	8
Phone No Names	8
Schedule Names	64
Door Group Names	16
Floor Group Names	32
PGM Names	250
Floor Names	128
Elevator Names	8
Elevator Floor Groups	32
Elevator Cars	8
Elevator Floor	1024
Programmable Function	64
Elevator Car Groups	8
Elevator Car Group Names	8
Analog Expander	8
Variable	248
Bit Variable	248

Access Control Profile

The access control profile is built to have a larger number of doors and reader expansion modules for an access control intensive application. A large number of users and doors as well as a reasonable amount of security provide the ideal access control and burglary integration profile.

Description	Number
LCD Keypad Modules (PRT-KLCD)	16
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	8
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	64
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	8

Description	Number
Zone Inputs	720
Trouble Zone Inputs	1408
PGM Outputs	772
PGM Groups	128
Area Groups	32
Menu Groups	16
Door Groups	248
Keypad Groups	16
Areas	32
Access Levels	248
Zone Types	128
Doors	128
Door Types	8
Services	8
Phone Numbers	16
Schedules	248
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	32
Panel Configuration Information	1
Users	10000
Events	4000
User Names	2000
Area Names	32
Access Level Names	248
Zone Type Names	64
Zone Input Names	720
Home Names	8
Door Names	128
Door Type Names	8
Area Group Names	32
Menu Group Names	16
Keypad Group Names	8
Phone No Names	8
Schedule Names	248
Door Group Names	248
Floor Group Names	32

Description	Number
PGM Names	16
Floor Names	128
Elevator Names	8
Elevator Floor Groups	32
Elevator Cars	8
Elevator Floor	1024
Programmable Function	64
Elevator Car Groups	8
Elevator Car Group Names	8
Analog Expander	8
Variable	248
Bit Variable	248

Elevator System Profile

The elevator system profile is built to have a larger number of elevator cars for an access control system that involves a large amount of elevator security, ideally suited to high rise apartment and office building configurations.

Description	Number
LCD Keypad Modules (PRT-KLCD)	8
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	4
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	32
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	8
Zone Inputs	368
Trouble Zone Inputs	800
PGM Outputs	468
PGM Groups	128
Area Groups	64
Menu Groups	16
Door Groups	128
Keypad Groups	8
Areas	64
Access Levels	248
Zone Types	32
Doors	64
Door Types	8
Services	8
Phone Numbers	16

Description	Number
Schedules	248
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	32
Panel Configuration Information	1
Users	2000
Events	2000
User Names	2000
Area Names	64
Access Level Names	248
Zone Type Names	32
Zone Input Names	368
Home Names	16
Door Names	16
Door Type Names	8
Area Group Names	64
Menu Group Names	16
Keypad Group Names	8
Phone No Names	8
Schedule Names	32
Door Group Names	16
Floor Group Names	128
PGM Names	16
Floor Names	128
Elevator Names	8
Elevator Floor Groups	128
Elevator Cars	16
Elevator Floor	2048
Programmable Function	32
Elevator Car Groups	16
Elevator Car Group Names	16
Analog Expander	8
Variable	248
Bit Variable	248

School Profile

The school profile is built to have a larger number of zone expansion devices for the significant increase in burglary requirements for education facilities.

Description	Number
LCD Keypad Modules (PRT-KLCD)	8
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	32
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	16
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	8
Zone Inputs	688
Trouble Zone Inputs	768
PGM Outputs	452
PGM Groups	128
Area Groups	64
Menu Groups	16
Door Groups	32
Keypad Groups	8
Areas	64
Access Levels	32
Zone Types	128
Doors	16
Door Types	8
Services	8
Phone Numbers	16
Schedules	128
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	32
Panel Configuration Information	1
Users	2000
Events	4000
User Names	2000
Area Names	64
Access Level Names	32
Zone Type Names	128
Zone Input Names	688
Home Names	16
Door Names	16
Door Type Names	8

Description	Number
Area Group Names	64
Menu Group Names	16
Keypad Group Names	8
Phone No Names	8
Schedule Names	32
Door Group Names	16
Floor Group Names	16
PGM Names	16
Floor Names	0
Elevator Names	16
Elevator Floor Groups	16
Elevator Cars	8
Elevator Floor	1024
Programmable Function	32
Elevator Car Groups	8
Elevator Car Group Names	8
Analog Expander	8
Variable	248
Bit Variable	248

Storage Profile

The storage profile is built to have a larger number of zone expansion devices but also caters for the significantly higher number of areas required to manage a storage locker or container facility. A smaller number of users and user names increases the memory for other functions, area groups and PGM groups.

Description	Number
LCD Keypad Modules (PRT-KLCD)	8
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	64
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	8
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	32
Zone Inputs	624
Trouble Zone Inputs	832
PGM Outputs	772
PGM Groups	248
Area Groups	248
Menu Groups	16
Door Groups	16
Keypad Groups	8

Description	Number
Areas	128
Access Levels	248
Zone Types	248
Doors	16
Door Types	8
Services	4
Phone Numbers	8
Schedules	64
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	16
Panel Configuration Information	1
Users	500
Events	4000
User Names	500
Area Names	128
Access Level Names	248
Zone Type Names	248
Zone Input Names	1136
Home Names	16
Door Names	16
Door Type Names	8
Area Group Names	248
Menu Group Names	16
Keypad Group Names	8
Phone No Names	8
Schedule Names	64
Door Group Names	16
Floor Group Names	16
PGM Names	16
Floor Names	0
Elevator Names	8
Elevator Floor Groups	16
Elevator Cars	8
Elevator Floor	1024
Programmable Function	128
Elevator Car Groups	8

Description	Number
Elevator Car Group Names	8
Analog Expander	8
Variable	248
Bit Variable	248

Automation Profile

The automation profile has a large number of automation points that are used in the system to allow control of large automation functionality in a building or residence. This also allows the assignment of certain automation functions for the control of external actions within programmable functions.

Description	Number
LCD Keypad Modules (PRT-KLCD)	32
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	8
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	32
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	8
Zone Inputs	528
Trouble Zone Inputs	1088
PGM Outputs	612
PGM Groups	128
Area Groups	64
Menu Groups	16
Door Groups	16
Keypad Groups	8
Areas	64
Access Levels	64
Zone Types	64
Doors	64
Door Types	8
Services	8
Phone Numbers	8
Schedules	32
Holidays	32
Daylight Saving Adjustment Settings	1
Automation Points	248
Panel Configuration Information	1
Users	2000
Events	1000
User Names	2000

Description	Number
Area Names	64
Access Level Names	64
Zone Type Names	16
Zone Input Names	528
Home Names	16
Door Names	4
Door Type Names	4
Area Group Names	248
Menu Group Names	16
Keypad Group Names	4
Phone No Names	8
Schedule Names	32
Door Group Names	4
Floor Group Names	4
PGM Names	16
Floor Names	0
Elevator Names	0
Elevator Floor Groups	0
Elevator Cars	8
Elevator Floor	1024
Programmable Function	128
Elevator Car Groups	8
Elevator Car Group Names	8
Analog Expander	16
Variable	248
Bit Variable	248

Apartment Profile

The apartment profile has a large number of keypad modules to cater for the condominium and apartment type installations. Ideally this profile would be used in conjunction with the ELT-KLCD keypad to provide complete independent control over any apartment.

Description	Number
LCD Keypad Modules (PRT-KLCD)	248
16 Zone Input Expanders (PRT-ZX16 and PRT-ZXS16)	4
2 Door Reader Expanders (PRT-RDM2, PRT-RDI2 and PRT-RDE2)	4
16 PGM Output Expanders (PRT-ZX16 and PRT-ZXS16)	2
Zone Inputs	1104

Description	Number
Trouble Zone Inputs	2224
PGM Outputs	1108
PGM Groups	128
Area Groups	248
Menu Groups	16
Door Groups	16
Keypad Groups	8
Areas	248
Access Levels	16
Zone Types	16
Doors	4
Door Types	4
Services	4
Phone Numbers	8
Schedules	32
Holidays	8
Daylight Saving Adjustment Settings	1
Automation Points	8
Panel Configuration Information	1
Users	2000
Events	2000
User Names	2000
Area Names	248
Access Level Names	16
Zone Type Names	16
Zone Input Names	1104
Home Names	16
Door Names	4
Door Type Names	4
Area Group Names	248
Menu Group Names	16
Keypad Group Names	4
Phone No Names	8
Schedule Names	32
Door Group Names	4
Floor Group Names	0
PGM Names	4

Description	Number
Floor Names	0
Elevator Names	0
Elevator Floor Groups	0
Elevator Cars	0
Elevator Floor	0
Programmable Function	0
Elevator Car Groups	0
Elevator Car Group Names	0
Analog Expander	8
Variable	248
Bit Variable	248

Data Register Definitions

Memory registers are locations of memory that can be used to store information, calculate information or provide links to the analog values from the PRT-ADC4 and PRT-DAC4 analog control modules. Memory registers can be used as part of programmable functions to perform actions and calculations and are access either in a Boolean Mode (Bits) or Data Mode (Word Value).

A memory register can refer to a decimal value from 0-65,535. When used in programmable functions a memory register will hold either a 0 or 1 in the appropriate bit or a value from 0-65,535.

Read/Write Memory Registers

Read and write general memory registers can be used to perform logic actions or other functions and are global throughout the Protege system controller.

Memory Register	Description	Type
MR00000	General Purpose Memory Register MR00000 can be used in any location.	Boolean Values 0 and 1 and decimal values up to 4,294,836,225.
MR00250	General Purpose Memory Register MR00250 can be used in any location.	Boolean Values 0 and 1 and decimal values up to 4,294,836,225.

Object Notation

When selecting an address for a module or an object (Zone, Trouble Zone or PGM) on a module the address is entered using the Module Type, Module Address and optionally the number of the object. This is referred to as the Protege Object Notation.

This notation allows fast and efficient access to any programmable or controllable object within the Protege System.

Notation Structure

Protege Object Notation always begins with the module type or system type defined by 2 letters and then followed by an address (3 digits). This is a requirement and is called the Unique Address. It is optionally followed by a 2 digit number that selects the object within the unique address such as a Zone or PGM and is separated by a colon.

ZX003:08

The above example refers to ZX (Zone Expansion Module) device address 003 and object 08. This could be PGM (programmable output) 8, Zone 8, or Trouble Zone 8 depending on the location that has been selected from keypad menu.

SC001

The example refers to SC (schedule) record address 001.

Module Object Type

The following list shows the module types. All module types have a two letter definition that is used to identify them in the system.

Module Type	Description
CP	Control Panel
KP	LCD Keypad
ZX	Zone Expander
PX	PGM Expander
RD	Reader Expander
AE	Analog Expander (Input or Output)

There are a number of products that utilize the same module object type. For example the PRT-RDM2 Mini Reader Expander still uses the module type RD as does the PRT-RDI2 and PRT-RDE2 however the hardware functionality is different when installed and the registered module type is displayed by pressing the **[ARM]** key at the expander selection screen.

System Object Type

All programmable system objects and functions have a two letter type definition associated with them. For example to program a user the user will always be prefixed with the two letter UN system object type identifier.

System Type	Description
UN	User Number
KP	LCD Keypad

System Type	Description
ZX	Zone Expander
PX	PGM Expander
RD	Reader Expander
ZN	Zone Input
TZ	Trouble Zone
PM	PGM Output
AG	Area Group
MG	Menu Group
DG	Door Group
KG	Keypad Group
AR	Area
AL	Access Level
ZT	Zone Type
DR	Door
DT	Door Type
SV	Service
PH	Phone Number
SC	Schedule
HL	Holiday
DL	Daylight Savings
AT	Automation
PL	Panel Configuration
EV	Event
FG	Floor Group
EL	Elevator
EF	Elevator Floor
FN	Programmable Function
EG	Elevator Group
AE	Analog Expander
DV	Data Variable
BV	Bit Variable
DS	Door Group Schedule
FS	Floor Group Schedule
UNT	User Number Name
ART	Area Name
ALT	Access Level Name
ZTT	Zone Type Name

System Type	Description
ZNT	Zone Name
ATT	Automation Name
DRT	Door Name
DTT	Door Type Name
AGT	Area Group Name
MGT	Menu Group Name
KGT	Keypad Group Name
PHT	Phone Number Name
SCT	Schedule Name
DGT	Door Group Name
FGT	Floor Group Name
PMT	Panel Name
FLT	Floor Name
ELT	Elevator Name

Data Entry

When programming the Protege System using the LCD Keypad the information is entered using predefined methods, these include List Entry (a list of predefined values or values looked up from another record), Decimal Entry, PGM and PGM Group, Protege Notation and Module Notation. Each of these entry methods use predefined keys and functions as outlined in the following sections.

Decimal Data Entry

Decimal numbers are entered using the 0-9 keys. Pressing the [STAY] key will set the minimum value, pressing the [FORCE] key will set the maximum value and pressing the [ARM] will recall the value that was previously set.

Decimal entry can take on any number of digits from 1 up to 32 depending on the location that the number is being entered. In the following example a number of 120 is being entered in to the door unlock time.

```
DR001 Unlock
time: 120 secs
```

When you enter in to a decimal entry screen the cursor will be located on the first decimal digit that can be set. For our example the default door time is 005 seconds however we want to set the unlock time to 120.

```
DR001 Unlock
time: 005 secs
```

In the above screen the cursor will be flashing over the first 0 of the 005 press the [1] key, the 0 will be replaced with a 1 and the cursor will move to the right over the next 0.

```
DR001 Unlock
time: 105 secs
```

Pressing the [2] will replace the 0 with a 2 and then the cursor will move to the right once again and be positioned over the 5 now press the [0] and the completed value will be seen on the screen of 120 as shown below.

```
DR001 Unlock
time: 120 secs
```

Once the information is entered as above the data is not saved until you move to another screen. Once you have moved off the screen by pressing the [ENTER] key or pressing the right, left, up or down key the data is saved.

If you have not moved off the screen and want to recall the previous setting you can press the [ARM] key to recall the currently set value.

Name and Text Data Entry

Many of the records within the Protege System can have an assigned name or text. As and example users, zones, areas and many other records have an associated text name that is used in the Protege System.

Programming the name or text value is completed using the numerical keys on the keypad in the same manner that you select a name or store a name using a mobile telephone keypad.

Entering text data is done by pressing keys multiple times to show the character required. The display will change as the key is pressed.

Using the character key map shown, to enter the name John, the [5] key is pressed once, move the cursor one location to the right with the [➔] key. Press the [6] key seven times and repeat the procedure for the other characters in the text entry.

Access Code and PIN Number Entry

Access codes or PIN numbers are entered using the 0-9 keys. Pressing the [DISARM] key will delete the PIN number.

PIN number entry can take on any number of digits from 1 up to 8 and can be preceded by any number of zeros. For example the codes 1, 01 and 0001 are all unique within the Protege System.

In the following example the user code 2580 is programmed for UN00003 (Demo User by Default) over writing the default demo user code of 111111.

```
UN00001 User
code: 111111
```

When you enter in to the PIN number entry screen the cursor will be located on the first programmed digit of the PIN number or if the PIN number is not set it will be at the first position available. For our example the demo user default PIN number of 111111 is going to be replaced with 2580.

```
UN00001 User
code: 111111
```

In the above screen the cursor will be flashing over the first 1 in the PIN number. We need to erase the PIN number that is currently programmed by pressing the [DISARM] key.

```
UN00001 User
code: _
```

Pressing the [2], [5], [8], [0] will insert the new PIN number in the location we just cleared using the [DISARM] key.

```
UN00001 User
code: 2580_
```

To save the PIN number press the [ENTER] key or use another navigation key to move off the screen and the number will be automatically saved.

If you have not moved off the screen and want to recall the previous PIN number setting you can press the [ARM] key.

Date and Time Data Entry

Date and time entries are used widely in the Protege System when configuring Schedules, Users and general configuration parameters.

In some cases to disable a feature that is related to a date or time entry the actual date and time field is used to activate the function that it provides. For example in the panel test report time screen a time configuration set to –-:-- will result in the test report being disabled.

To clear the time or date setting press the [DISARM] key. The display will show the --:-- for the time and --/--/---- for the date entry.

```
Test report
time: 02:00
```

In the example below we will be setting the test report time in the panel configuration section to 3:30pm. The Protege accepts entries for all programmable time and date information in military format. Display of the time on the LCD display can be configured for a 12 hour clock however this is a display feature only.

```
Test report
time: 02:00
```

The cursor will be located on the first digit of the hour field. Press the [1] key to program the first digit followed by the [5], [3] and [0]. The display will now show 15:30 on the screen as below.

```
Test report
time: 15:30
```

The new value will be programmed when the [ENTER] key is pressed or another navigation key is pressed moving screens.

Hexadecimal Data Entry

Hexadecimal entry is required in only a few key locations however it is an important part of the data entry process. Use the 0-9 keys for the numerical data portion and the 2 and 3 key to obtain the letters A-F (Press the 2 and 3 keys multiple times to cycle through the available values A, B,C and D, E, F).

Pressing the [STAY] key will set the minimum value, pressing the [FORCE] key will set the maximum value and pressing the [ARM] will recall the value that was previously set.

Hexadecimal entry can take on any number of digits from 1 up to 32 depending on the location that the hexadecimal number is being entered. In the following example a number of 21B64C90 is being entered in to the host id setting in the panel configuration.

```
Panel host
ID: 00000000
```

When you enter in to a hexadecimal entry screen the cursor will be located on the first hexadecimal digit that can be set. For our example the default host id of 00000000 will be replaced with our new host id of 21B64C90.

The arrow keys (left and right) can be used to move the cursor to the desired position in the hexadecimal number if only one part of the existing value requires modification. For example to program a host id of 00000001 you can right arrow to the last digit and simply press the [1] key to set the digit.

```
Panel host
ID: 00000000
```

In the above screen the cursor will be flashing over the first 0 of the 00000000 press the [2] key, the 0 will be replaced with a 2. The cursor will NOT move to the right automatically you must press the right arrow key. Repeat the above procedure for the 1 value pressing the right arrow key when done.

```
Panel host
ID: 21B00000
```

When entering the B press the [2] key 3 times and the display will show the B at the third position pressing the right arrow once the B is shown in the display. Repeat the same procedures above for the remainder of the value.

```
Panel host
ID: 21B64C90
```

Press the [ENTER] key to save the value shown.

List Data Entry

List data entry is used through out the Protege System and is styled similar to the drop down combination boxes you find in most computer systems. Data is presented in a list of selectable values. These values may be from another programmed record in the system (Schedules as an example) or from a predefined static set of values (Card Reader Formats as an example).

Pressing the [DISARM] key will set the list data entry to the none selection, pressing the [ARM] will recall the value that was previously set.

List entries are scrolled using the [1] and [3] keys. Pressing the [1] key will move the display up the list and pressing the [3] key will move down the list. In our example we want to select the 4th schedule for the access level is programmed as *Schedule 004.

```
AL001 Schedule
Working Hours
```

The list entry does not have a cursor as the display shows a fixed value from a static table or internal record. In our example the display is from the access level schedule selection and the list data entry is used to select the schedule that the access level will use to operate.

To change this to the value that we want of *Schedule 004 you would simply press the [1] key three times moving the display to *Schedule 004. Once this is displayed we can save the setting by pressing the [ENTER] key.

Option Select Entry

Option selection screens are used to enable and disable settings in the Protege System. An option selection is a Yes/No setting that is presented in blocks of 8. You can also select the option using text entry by pressing the [STAY] key and then using the [🡻] and [🡹] arrow keys to scroll through the options pressing the [1] key to toggle the option on or off.

Changing an option is done using the keys [1] to [8]. Pressing the [ARM] key will recall the current option settings. In our example we will modify the general options for the reader expander.

```
RD001 General
   [********]
```

The list entry does not have a cursor, to toggle an option on or off press the appropriate key from [1] to [8]. For example to turn on option 2 (Multiple Reader Input Port 1) press the [2] key. As shown below the 2 will now replace the '*' character. A '*' indicates that the option is disabled while a numerical number at the location indicates that the option is enabled or on.

```
RD001 General
   [*2******]
```

Options can also be view in text mode this is entered by pressing the [STAY] key while the options screen is displayed. The screen will change to text mode as shown below with the first option displayed.

```
1. Set battery
charge 700mA: N
```

To change this option press the [1] key or to scroll the options press the [🡻] and [🡹] arrow keys. To return to the options screen press the [STAY] key. To save the options move off the screen using a navigation key or press the [ENTER] key.

PGM and PGM Group Entry

PGM and PGM Group Entry is done by selecting the module type and then the address and actual PGM number on the device. For example to program the second lock output on the fourth reader expander you would enter RD004:02 where the RD is entered using the ascii mode similar to the text entry and the 004 and 02 are entered using normal decimal mode entry.

In the following example we will program the Green LED on the LCD keypad at address 001 to activate when the area is disarmed. We program this option in the area configuration.

```
AR001 Disarmed
pgm: --000:00
```

In the above screen the default value for a PGM is shown this is –000:00. To default the PGM entry press the [DISARM] key or to recall the currently programmed value press the [ARM] key. Pressing the [5] key twice will put a 'K' in the first location. Using the table in the Object Notation Section (see page 330) the keypad is referenced as a KP. Press the [➔] arrow key to move to the next location.

```
AR001 Disarmed
pgm: K-000:00
```

Pressing the [7] key once will show the 'P' on the screen, move the cursor to the right using the [➔] key.

```
AR001 Disarmed
pgm: KP000:00
```

Complete the entry by pressing **[0]**, **[0]**, **[1]** then the PGM output number by pressing **[0]** and **[3]** for the green LED.

To enter a PGM group complete the same procedures as above however use the PG for the prefix in the module type, the screen will change to only have 3 digits allowing the PGM group to be entered. See below for an example of PGM group 4 at the same location as above.

```
AR001 Disarmed
pgm: PG004
```

Zone Entry

Zone entry is done by selecting the module type and then the address and actual zone number on the device. For example to program the second zone on the fourth zone expander you would enter ZX004:02 where the ZX is entered using the ascii mode similar to the text entry and the 004 and 02 are entered using normal decimal mode entry.

In the following example we will program zone 6 on the Zone Expander at address 003 to be the REX Zone for the Virtual Door.

```
FN001 REX
zone --000:00
```

In the above screen the default value for a zone is shown this is --000:00. To default the zone entry press the **[DISARM]** key or to recall the currently programmed value press the **[ARM]** key. Pressing the **[9]** key 4 times will put a 'Z' in the first location. Using the table in the Object Notation Section (see page 330) the zone expander is referenced as a ZX. Press the **[➔]** arrow key to move to the next location.

```
FN001 REX
zone Z-000:00
```

Pressing the [9] key twice will show the 'X' on the screen, move the cursor to the right using the [➔] key.

```
FN001 REX
zone ZX000:00
```

Complete the entry by pressing **[0]**, **[0]**, **[3]** then the PGM output number by pressing **[0]** and **[6]** for zone 6.

Conversion

When programming the Protege System it is required in some instances that a value be converted from Hexadecimal. ASCII or Decimal for entry in to a specific field. The following tables allow a quick look up of the conversion and associated values.

Hexadecimal Conversion

In some cases it is required that you convert a hexadecimal character in to a decimal character. The following table can be used to convert between the base 16 (Hexadecimal) and base 10 (Decimal) number systems.

DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX
000	00	064	40	128	80	192	C0
001	01	065	41	129	81	193	C1
002	02	066	42	130	82	194	C2
003	03	067	43	131	83	195	C3
004	04	068	44	132	84	196	C4
005	05	069	45	133	85	197	C5
006	06	070	46	134	86	198	C6
007	07	071	47	135	87	199	C7
008	08	072	48	136	88	200	C8
009	09	073	49	137	89	201	C9
010	0A	074	4A	138	8A	202	CA
011	0B	075	4B	139	8B	203	CB
012	0C	076	4C	140	8C	204	CC
013	0D	077	4D	141	8D	205	CD
014	0E	078	4E	142	8E	206	CE
015	0F	079	4F	143	8F	207	CF
016	10	080	50	144	90	208	D0
017	11	081	51	145	91	209	D1
018	12	082	52	146	92	210	D2
019	13	083	53	147	93	211	D3
020	14	084	54	148	94	212	D4
021	15	085	55	149	95	213	D5
022	16	086	56	150	96	214	D6
023	17	087	57	151	97	215	D7
024	18	088	58	152	98	216	D8
025	19	089	59	153	99	217	D9
026	1A	090	5A	154	9A	218	DA
027	1B	091	5B	155	9B	219	DB

DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX
028	1C	092	5C	156	9C	220	DC
029	1D	093	5D	157	9D	221	DD
030	1E	094	5E	158	9E	222	DE
031	1F	095	5F	159	9F	223	DF
032	20	096	60	160	A0	224	E0
033	21	097	61	161	A1	225	E1
034	22	098	62	162	A2	226	E2
035	23	099	63	163	A3	227	E3
036	24	100	64	164	A4	228	E4
037	25	101	65	165	A5	229	E5
038	26	102	66	166	A6	230	E6
039	27	103	67	167	A7	231	E7
040	28	104	68	168	A8	232	E8
041	29	105	69	169	A9	233	E9
042	2A	106	6A	170	AA	234	EA
043	2B	107	6B	171	AB	235	EB
044	2C	108	6C	172	AC	236	EC
045	2D	109	6D	173	AD	237	ED
046	2E	110	6E	174	AE	238	EE
047	2F	111	6F	175	AF	239	EF
048	30	112	70	176	B0	240	F0
049	31	113	71	177	B1	241	F1
050	32	114	72	178	B2	242	F2
051	33	115	73	179	B3	243	F3
052	34	116	74	180	B4	244	F4
053	35	117	75	181	B5	245	F5
054	36	118	76	182	B6	246	F6
055	37	119	77	183	B7	247	F7
056	38	120	78	184	B8	248	F8
057	39	121	79	185	B9	249	F9
058	3A	122	7A	186	BA	250	FA
059	3B	123	7B	187	BB	251	FB
060	3C	124	7C	188	BC	252	FC
061	3D	125	7D	189	BD	253	FD
062	3E	126	7E	190	BE	254	FE
063	3F	127	7F	191	BF	255	FF

ASCII Conversion

In some cases it is required that you convert a ASCII (American Standard Character for Information Interchange) character in to a decimal or hexadecimal character. The following table can be used to convert between the ASCII character and the equivalent hexadecimal or decimal value.

ASCII	DEC	HEX	ASCII	DEC	HEX
NUL	000	00	@	64	40
SOH	001	01	A	65	41
STX	002	02	B	66	42
ETX	003	03	C	67	43
EOT	004	04	D	68	44
ENQ	005	05	E	69	45
ACK	006	06	F	70	46
BEL	007	07	G	71	47
BS	008	08	H	72	48
TAB	009	09	I	73	49
LF	010	0A	J	74	4A
VT	011	0B	K	75	4B
FF	012	0C	L	76	4C
CR	013	0D	M	77	4D
SO	014	0E	N	78	4E
SI	015	0F	O	79	4F
DLE	016	10	P	80	50
DC1	017	11	Q	81	51
DC2	018	12	R	82	52
DC3	019	13	S	83	53
DC4	020	14	T	84	54
NAK	021	15	U	85	55
SYN	022	16	V	86	56
ETB	023	17	W	87	57
CAN	024	18	X	88	58
EM	025	19	Y	89	59
SUB	026	1A	Z	90	5A
ESC	027	1B	[	91	5B
FS	028	1C	\	92	5C
GS	029	1D	]	93	5D
RS	030	1E	^	94	5E
US	031	1F	_	95	5F
SPACE	032	20	`	96	60

ASCII	DEC	HEX	ASCII	DEC	HEX
!	033	21	a	97	61
"	034	22	b	98	62
#	035	23	c	99	63
$	036	24	d	100	64
%	037	25	e	101	65
&	038	26	f	102	66
'	039	27	g	103	67
(	040	28	h	104	68
)	041	29	i	105	69
*	042	2A	j	106	6A
+	043	2B	k	107	6B
,	044	2C	l	108	6C
-	045	2D	m	109	6D
.	046	2E	n	110	6E
/	047	2F	o	111	6F
0	048	30	p	112	70
1	049	31	q	113	71
2	050	32	r	114	72
3	051	33	s	115	73
4	052	34	t	116	74
5	053	35	u	117	75
6	054	36	v	118	76
7	055	37	w	119	77
8	056	38	x	120	78
9	057	39	y	121	79
:	058	3A	z	122	7A
;	059	3B	{	123	7B
<	060	3C	|	124	7C
=	061	3D	}	125	7D
>	062	3E	~	126	7E
?	063	3F	DEL	127	7F

Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (http://www.incontrol.co.nz) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

11 Canaveral Drive
Albany
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Fax: +64-9-476-7128

Email: sales@incontrol.co.nz or support@incontrol.co.nz

Web: www.incontrol.co.nz

Integrated Control Technology Limited

11 Canaveral Drive, Albany, Auckland 0632
P.O. Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: support@incontrol.co.nz Phone: +64 (9) 476 7124 **Fax:** +64 (9) 476 7128
Designers & manufacturers of integrated electronic access control, security & automation products.
Designed & manufactured by Integrated Control Technology Limited.
Copyright © Integrated Control Technology Limited 2003-2011. All rights reserved.

www.incontrol.co.nz

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees, shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice.

227-4045-500